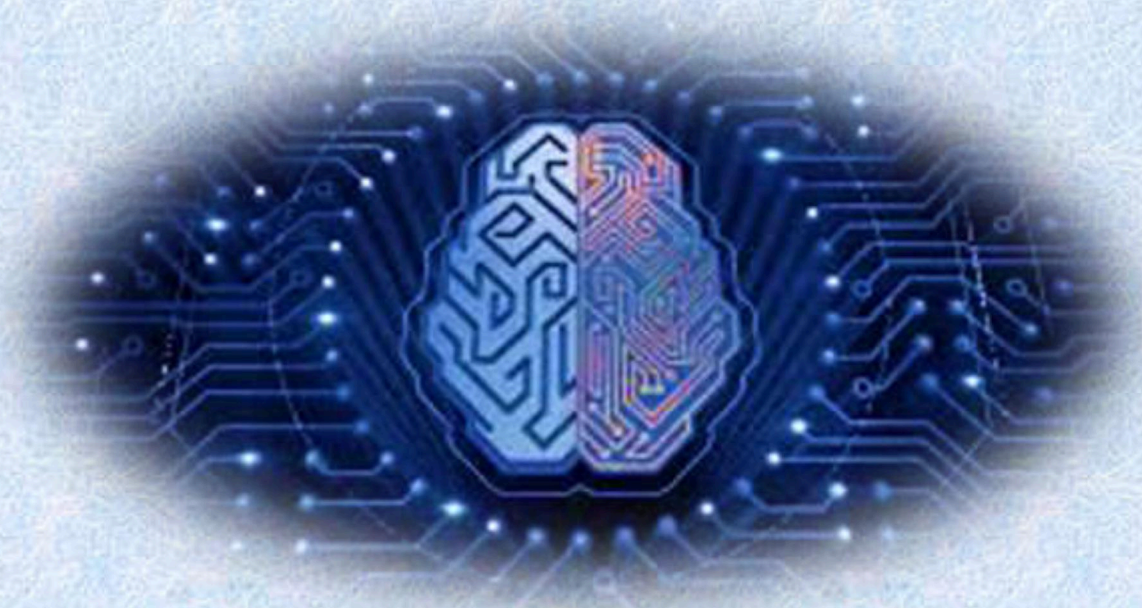
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ

«ГЛАВНЫЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЙ ЦЕНТР»



Обзор

отдельных вопросов

в области больших данных и искусственного интеллекта

IV ВЫПУСК

том 1

Москва 2020

Под общей редакцией В.С. Овчинского,
доктора юридических наук,
советника Министра внутренних дел
Российской Федерации

Обзор отдельных вопросов в области
больших данных и искусственного интеллекта.
IV выпуск, 1 том.
М.: ФКУ «ГИАЦ МВД России», 2020. – 626 с.

В обзоре представлены материалы, касающиеся вопросов использования больших данных и развития искусственного интеллекта в мире. Отдельно отражены актуальные вопросы использования ИИ в правоохранительной системе.

Оглавление

Распоряжение Правительства РФ от 19.08.2020 N 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года» 6

I. Общие положения 7

II. Общеотраслевые задачи регулирования применения технологий искусственного интеллекта и робототехники 14

III. Отраслевые направления совершенствования регулирования применения технологий искусственного интеллекта и робототехники 24

IV. Регуляторные меры для финансового стимулирования развития отрасли 33

V. Механизмы реализации Концепции 33

На пути к инновациям в области ИИ 36

Второй доклад об искусственном интеллекте для правоохранительных органов 36

1. Интеграция ии в правоохранительных органах 42

2. Области искусственного интеллекта 46

3. Опыт исспользования правоохранительными органами 54

4. Ответственность при исспользовании ии 61

5. Потребности и рекомендации для полиции 75

5. Ответственный инструмент ии на службе правоохранителей 77

6. Дорожная карта 80

Приложение I 81

Приложение II 84

Искусственный интеллект и правоохранительные органы 88

Общая информация 94

1. Цели и структура 96

2. Правовая основа ЕС 98

3. Применение законодательства и уголовное правосудие 109

4. Влияние на основные права 134

5. Разработка политики 146

6. Правоохранительные инициативы 179

7. Полностью оценить актуальность и пробелы в существующей правовой базе ... 181
Приложение 1. ... 203
Специальная коллекция по искусственному интеллекту ... 212
Краткий обзор ... 216
Уголовное право в области медицины и биологии ... 217
Уголовное право и появление искусственного интеллекта ... 221
Применение балансировочных тестов ... 226
Справедливость, доверие и технология лица в полисировании ... 234
Ограничение целей дизайном как против функциональной ползучести и системной безопасности в police ai ... 250
От доказательств к доказательствам: анализ социальных сетей в уголовных судах италии ... 272
Искусственный интеллект в здравоохранении: оценка рисков и уголовное право ... 290
Искусственный интеллект: deepfakes как пример вызовов ии системам уголовного правосудия ... 311
Аналитика на основе ИИ ... 338
Критерий 1 – Трансграничные потоки данных и локализация ... 360
Критерий 2 – Рамки защиты персональных данных и конфиденциальности ... 362
Критерий 3 – Цифровая промышленная политика ... 364
Критерий 4 – Исследования и разработки в области искусственного интеллекта (НИОКР) ... 366
Критерий 5 – Инфраструктура и развитие ... 368
Критерий 6 – Административный потенциал и регулирование ... 370
Критерий 7 – Лидерство и власть ... 372
Краткая типология ... 375
Таблица 1: Типологическая матрица режима данных ... 375
Вывод ... 375
Наблюдать и прогнозировать ... 387
Последствия для права на равенство и свободу от дискриминации: ... 398
Правовой анализ собранных данных ... 411
Социально-исторический контекст ... 411

Уголовное правосудие и системная дискриминация в Канаде 412
В фокусе внимания № 1 426
В фокусе внимания № 2 440
В фокусе внимания № 3 462
В фокусе внимания № 4 483
В фокусе внимания № 5 508
В фокусе внимания № 6 544
В фокусе внимания № 7 562
В фокусе внимания № 8 572
Алгоритмические оценки воздействия 572
Право на средство правовой защиты 576
Средства правовой защиты от нарушений прав человека должны быть эффективными 581
Заключительные комментарии: алгоритмическое наблюдение и право на средство правовой защиты 583
Подход к алгоритмической деятельности полиции, основанной на соблюдении прав человека 583
Рекомендации и заключение 584
Приоритетные рекомендации для алгоритмической работы полиции в Канаде 586
Вывод 612

Распоряжение Правительства РФ от 19.08.2020 N 2129-р «Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года»

1. Утвердить прилагаемую Концепцию развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года (далее – Концепция).

2. Федеральным органам исполнительной власти и Государственной корпорации по космической деятельности «Роскосмос» руководствоваться положениями Концепции при осуществлении функций по выработке государственной политики и нормативно-правовому регулированию в установленных сферах деятельности.

3. Заинтересованным федеральным органам исполнительной власти и Государственной корпорации по космической деятельности «Роскосмос» в 3-месячный срок представить в Минэкономразвития России предложения по реализации Концепции в рамках национальной программы «Цифровая экономика Российской Федерации».



Председатель Правительства

Российской Федерации

М. МИШУСТИН

Утверждена
распоряжением Правительства
Российской Федерации
от 19 августа 2020 г. № 2129-р

КОНЦЕПЦИЯ
РАЗВИТИЯ РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В СФЕРЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА И РОБОТОТЕХНИКИ ДО 2024 ГОДА

I. Общие положения

1. Цели Концепции

Целью Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники (далее – Концепция) является определение основных подходов к трансформации системы нормативного регулирования в Российской Федерации для обеспечения возможности создания и применения таких технологий в различных сферах экономики с соблюдением прав граждан и обеспечением безопасности личности, общества и государства.

Одновременно целями Концепции являются создание предпосылок для формирования основ правового регулирования новых общественных отношений, складывающихся в связи с разработкой и применением технологий искусственного интеллекта, робототехники и систем на их основе, а также определение правовых барьеров, препятствующих разработке и применению указанных систем.

Термины, используемые в настоящей Концепции, употребляются в значении, приведенном в Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (далее – Национальная стратегия), а также в национальных стандартах.

Развитие технологий искусственного интеллекта ставит серьезные вызовы перед правовой системой Российской Федерации, системой государственного управления и обществом в целом. Они обусловлены определенной степенью автономности действий систем искусственного интеллекта в решении поставленных задач и их неспособностью непосредственно воспринимать этические и правовые нормы, учитывать их при осуществлении каких-либо действий.

В настоящее время в Российской Федерации отсутствует специальное законодательное регулирование, учитывающее специфику применения технологий искусственного интеллекта и робототехники.

В то же время анализ мирового опыта показывает, что в целом ряде стран уже существует первичное правовое регулирование применения искусственного интеллекта и робототехники.

Концепция исходит из того, что для развития технологий искусственного интеллекта и робототехники необходимо создание регуляторной среды, комфортной для безопасного развития и внедрения указанных технологий, основанной на балансе интересов человека, общества, государства, компаний-разработчиков систем искусственного интеллекта и робототехники, а также потребителей их товаров, работ, услуг. Однако представления об этом балансе существенно разнятся. В связи с этим Концепция оставляет открытыми и требующими дальнейшего обсуждения отдельные наиболее спорные вопросы, но может служить инструментом для достижения в ближайшие годы сближения интересов человека, общества, государства и бизнеса в рассматриваемой сфере.

Концепция учитывает положения Национальной стратегии, национальной программы «Цифровая экономика Российской Федерации» и Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента Российской Федерации от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», а также положения иных документов стратегического планирования, нормативных правовых актов и методических документов, в том числе международных организаций.

С учетом динамики развития общественных отношений, связанных с созданием и использованием технологий искусственного интеллекта и робототехники, положения Концепции определены с перспективой на период до 2024 года.

2. Цели и задачи регулирования отношений в сфере технологий искусственного интеллекта и робототехники

Приоритетной целью регулирования отношений в сфере искусственного интеллекта и робототехники на данном этапе их развития является стимулирование разработки, внедрения и использования таких технологий, создания систем искусственного интеллекта и робототехники в доверенном и безопасном исполнении, которое будет способствовать достижению высоких темпов экономического роста, повышению благосостояния и качества жизни граждан, обеспечению национальной безопасности и правопорядка, достижению устойчивой конкурентоспособности российской экономики, в том числе лидирующих позиций в мире в области искусственного интеллекта.

С учетом заявленной цели регулирования выделяются следующие задачи, на решение которых должно быть направлено регулирование:

- создание основ правового регулирования новых общественных отношений, формирующихся в связи с применением систем искусственного интеллекта и робототехники, имеющих преимущественно стимулирующий характер;
- определение правовых барьеров, затрудняющих разработку и применение систем искусственного интеллекта и робототехники в различных отраслях экономики и социальной сферы;
- формирование национальной системы стандартизации и оценки соответствия в области технологий искусственного интеллекта и робототехники.

При этом режим правового регулирования разработки, внедрения и применения технологий и систем искусственного интеллекта и робототехники должен обеспечивать необходимую степень защиты прав и свобод человека и гражданина, отвечать интересам общества и государства.

3. Принципы регулирования отношений в сфере технологий искусственного интеллекта и робототехники

Достижение цели и задач регулирования отношений, складывающихся в связи с разработкой и применением систем искусственного интеллекта и робототехники, должно осуществляться с учетом следующих принципов:

- стимулирования развития технологий искусственного интеллекта и робототехники регуляторными средствами как основной вектор развития регулирования в обозначенный временной период («стимулирование как основа регулирования»);
- регуляторного воздействия, основанного на риск-ориентированном, междисциплинарном подходе и предусматривающее принятие ограничительных норм в случае, если применение технологий искусственного интеллекта и робототехники несёт объективно высокий риск причинения вреда участникам общественных отношений, правам человека и интересам общества и государства;
- расширения применения инструментов сорегулирования и саморегулирования, формирования кодексов (сводов) этических правил разработки, внедрения и применения технологий искусственного интеллекта и робототехники;
- человеко-ориентированного подхода, предусматривающего, что конечной целью развития технологий искусственного интеллекта и робототехники, направляемого посредством регуляторного воздействия, является обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека и повышение благосостояния и качества жизни граждан;
- оценки воздействия технологий и систем искусственного интеллекта и робототехники на все сферы жизни человека, общества и государства, основанная на научно выверенных исследованиях с подключением широкого круга ученых;
- обеспечения баланса интересов разработчиков, потребителей и иных лиц в сфере искусственного интеллекта и робототехники, а также определения границ их ответственности за возможные негативные последствия использования технологий искусственного интеллекта и робототехники;

- технологического суверенитета, предусматривающего обеспечение необходимого уровня независимости Российской Федерации в области искусственного интеллекта и робототехники с учетом государственной политики в сфере развития информационных технологий и импортозамещения;

- поддержки конкуренции, предусматривающей обеспечение равных для всех, включая предприятия малого и среднего бизнеса, возможностей для применения экспериментальных правовых режимов и мер государственной поддержки, а также для доступа к необходимым в целях разработки систем искусственного интеллекта и робототехники данным из государственных и муниципальных информационных систем;

- оценки при разработке нормативных правовых актов и иных документов в сфере искусственного интеллекта и робототехники социально-экономических последствий и рисков в условиях постоянного развития технологий, учет как положительного, так и отрицательного международного опыта регулирования;

- обязательности обоснованной оценки рисков причинения при применении искусственного интеллекта и робототехники вреда жизни и здоровью человека, реализации угроз обороне страны и безопасности государства и принятие мер, направленных на минимизацию таких рисков и угроз.

Развитие технологий искусственного интеллекта и робототехники должно основываться на базовых этических нормах и предусматривать:

- приоритет благополучия и безопасности человека, защиты его основополагающих прав и свобод (цель обеспечения благополучия и безопасности человека должна преобладать над иными целями разработки и применения систем искусственного интеллекта и робототехники);

- запрет на причинение вреда человеку по инициативе систем искусственного интеллекта и робототехники (по общему правилу следует ограничивать разработку, оборот и применение систем искусственного интеллекта и робототехники, способных по своей инициативе целенаправленно причинять вред человеку);

- подконтрольность человеку (в той мере, в которой это возможно с учетом требуемой степени автономности систем искусственного интеллекта и робототехники и иных обстоятельств);

- проектируемое соответствие закону, в том числе требованиям безопасности (применение систем искусственного интеллекта не должно заведомо для разработчика приводить к нарушению правовых норм);

- недопущение противоправной манипуляции поведением человека.

4. Проблемы, общие подходы и направления регулированияотношений в сфере технологий искусственного интеллектаи робототехники

Одним из основных препятствий для расширения применения систем с использованием искусственного интеллекта и робототехники является отсутствие достаточной степени доверия к ним со стороны общества. Повышение степени автономности таких систем, снижение контроля человека за процессом их применения, не полностью прозрачный процесс принятия решений создают общественный запрос на регуляторные ограничения применения систем искусственного интеллекта и робототехники.

В настоящее время в мире отсутствуют единые подходы к регулированию технологий искусственного интеллекта и робототехники, что связано с наличием ряда проблем, не имеющих однозначного решения.

Среди таких концептуальных проблемных направлений регулирования можно выделить следующие:

- соблюдение баланса между требованиями по защите персональных данных и необходимостью их использования для обучения систем искусственного интеллекта;
- определение предмета и границ регулирования сферы использования систем искусственного интеллекта и робототехники;
- идентификация системы искусственного интеллекта при взаимодействии с человеком, включая его информирование о взаимодействии с такой системой;
- правовое «делегирование» решений системам искусственного интеллекта и робототехники;
- ответственность за причинение вреда с использованием систем искусственного интеллекта и робототехники;
- правовой режим результатов интеллектуальной деятельности, созданных с использованием систем искусственного интеллекта;
- использование для принятия решений системами искусственного интеллекта вероятностных оценок и невозможность в ряде случаев полного объяснения, принятого ими решения (проблема алгоритмической прозрачности систем искусственного интеллекта).

Такие направления регулирования и указанные в пункте 49 Национальной стратегии основные направления создания комплексной системы регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий искусственного интеллекта, должны стать основными ориентирами при создании комплексной системы регулирования общественных отношений, возникающих в связи с развитием и внедрением технологий искусственного интеллекта и робототехники.

С учетом экономической и социальной значимости применения технологий искусственного интеллекта и робототехники в различных сферах их разработка и эксплуатация не должны ограничиваться регуляторными мерами, за исключением случаев, связанных с высоким риском причинения вреда жизни и здоровью граждан. Также не допускается применение технологий искусственного интеллекта и робототехники, представляющих явную угрозу обороне страны и безопасности государства.

Для выработки конкретных регуляторных решений требуется использовать риск-ориентированный подход, основанный на оценке размера потенциального вреда указанным ценностям с учетом вероятности его наступления по сравнению с потенциальным положительным эффектом от внедрения технологий искусственного интеллекта и робототехники, необходимости принятия мер по минимизации соответствующих рисков.

Сам факт использования систем искусственного интеллекта и робототехники не должен являться основанием для установления регуляторных ограничений.

Следует поддерживать развитие регулирования, вырабатываемого и приводимого в исполнение силами участников рынка (саморегулирование), включая принятие и использование документов национальной системы стандартизации, кодексов (сводов) этических правил и иных документов саморегулируемых организаций, а также иных инструментов.

Учитывая принципиальную сложность регулируемой сферы правоотношений, для выработки режима регулирования технологий искусственного интеллекта и робототехники требуется активное вовлечение представителей компаний - разработчиков систем искусственного интеллекта и робототехники, научно-исследовательских организаций в процесс экспертной проработки соответствующих нормативных правовых актов.

В дальнейшем может также потребоваться уточнение отдельных норм законодательства в целях нормативного правового регулирования новых видов правоотношений.

II. Общеотраслевые задачи регулирования применения технологий искусственного интеллекта и робототехники

1. Создание механизмов упрощенного внедрения продуктов с использованием технологий искусственного интеллектаи робототехники

Требуется создать возможности для использования специального механизма тестирования (опытной эксплуатации) и последующего внедрения решений в сфере искусственного интеллекта и робототехники.

Такой механизм, в свою очередь, должен позволять своевременно эффективно внедрять разработки без неучитывающих их специфику избыточных административных процедур, без корректировки всего применимого законодательства и с обеспечением необходимого уровня безопасности и контролируемости со стороны государственных органов.

Перспективными инструментами создания такого механизма являются экспериментальные правовые режимы («регуляторные песочницы»), а применительно к промышленности – также правовой режим полигона общего доступа. Их применение соответствует лучшим мировым практикам и отвечает интересам индустрии. В краткосрочной перспективе требуется принятие соответствующих нормативных правовых актов, обеспечивающих гибкий механизм быстрого создания таких режимов:

- в максимально широком круге отраслей;
- с возможностью участия в них заинтересованных лиц на недискриминационных условиях;
- с возможностью последующего включения в законодательство Российской Федерации по результатам регуляторного эксперимента норм, необходимых для применения соответствующих технологий.

Применение экспериментальных правовых режимов будет востребовано в том числе для таких продуктов и решений, как отдельные системы искусственного интеллекта в здравоохранении, медицинская робототехника, системы искусственного интеллекта и робототехники специального и двойного назначения, системы искусственного интеллекта и робототехники в сфере транспорта и логистики, системы искусственного интеллекта в государственном управлении, отдельные инструменты финансового стимулирования развития сфер искусственного интеллекта и робототехники, системы искусственного интеллекта и робототехники для строительства и топливно-энергетического комплекса.

2. Юридическая ответственность в случае применения системискусственного интеллекта и робототехники

Наиболее значимыми вопросами применения систем искусственного интеллекта и робототехники в контексте гражданско-правовых отношений являются вопросы гражданско-правовой ответственности за вред, причиненный системами искусственного интеллекта и робототехники. Реальный уровень развития технологий искусственного интеллекта и робототехники не предполагает кардинальных изменений в регулировании института юридической ответственности, однако требует постепенной доработки его отдельных элементов.

Требуется дальнейшая проработка механизмов гражданско-правовой, уголовной и административной ответственности в случае причинения вреда системами искусственного интеллекта и робототехники, имеющими высокую степень автономности, при принятии ими решений, в том числе с точки зрения определения лиц, которые будут нести ответственность за их действия, доработки при необходимости механизмов безвиновной гражданско-правовой ответственности, а также возможности использования способов, позволяющих возместить причиненный действиями систем искусственного интеллекта и робототехники вред (например, страхование ответственности, создание компенсационных фондов и др.).

Также при наличии реального риска нарушения прав и свобод человека может быть актуальной проработка вопроса об условиях идентификации системы искусственного интеллекта при прямом взаимодействии с человеком.

Общий вектор возможных изменений должен быть направлен на то, чтобы гарантировать эффективное и справедливое функционирование институтов юридической ответственности и распределение ответственности в случае такого причинения вреда.

3. Совершенствование режима оборота данных

Увеличение объема доступных данных и развитие информационно-коммуникационной инфраструктуры для доступа к данным являются одними из основных факторов развития технологий искусственного интеллекта.

Законодательство Российской Федерации в области информации, информационных технологий и защиты информации направлено главным

образом на обеспечение режимов конфиденциальности информации и защиты персональных данных.

С учетом задачи повышения доступности и качества данных требуется адаптация законодательства Российской Федерации в целях обеспечения:

- благоприятных правовых условий для безопасного и ответственного доступа разработчиков систем искусственного интеллекта и робототехники к данным безопасного обмена различными типами данных, включая данные, собираемые государственными органами и медицинскими организациями;

- особых условий (режимов) для доступа к данным, включая персональные данные (при условии принятия мер для защиты интересов субъектов персональных данных, включая обезличивание), в целях проведения научных исследований, обучения искусственного интеллекта и разработки технологических решений на их основе, а также правовых условий для организации идентификации с использованием технологий искусственного интеллекта и робототехники (при условии соблюдения права человека на неприкосновенность частной жизни).

В связи с этим необходимо расширение практики раскрытия данных, содержащихся в информационных ресурсах органов и организаций государственного сектора, а также в информационных ресурсах, созданных в целях реализации полномочий органов и организаций государственного сектора (государственных данных). Целесообразно также заложить основы правового регулирования функционирования общедоступных платформ таких данных. Требуются нормативное расширение перечня и типов открытых указанных данных для целей их использования разработчиками в сфере искусственного интеллекта и закрепление соответствующих полномочий органов государственной власти.

В целях максимального использования потенциала «больших данных» требуется также изменение существующих подходов к регулированию обезличенных данных. При условии принятия правовых, организационных и технических мер для защиты прав субъектов персональных данных для обработки обезличенных данных должен быть предусмотрен более свободный правовой режим. Определение правил применения и оборота данных, полученных в результате обезличивания сведений, составляющих профессиональную и коммерческую тайну, будет способствовать большей доступности данных и стимулировать их владельцев к взаимовыгодному обмену.

Кроме того, для существующих режимов профессиональной тайны (врачебная тайна, банковская тайна, тайна связи, адвокатская тайна и др.)

необходимо проработать вопрос целесообразности и возможности определения условий, при которых субъекты профессиональной тайны вправе привлекать для обработки соответствующих сведений сторонние организации (в том числе для раскрытия потенциала облачных технологий и технологий с использованием искусственного интеллекта).

Целесообразно предусмотреть уточнение правил получения согласия на обработку персональных данных для случаев, когда такая обработка осуществляется при проведении научных исследований в сфере искусственного интеллекта (например, в сфере здравоохранения, экологии, социологии и др.) и его обучения, а также использовать системы искусственного интеллекта, обеспечивающие необходимый уровень защиты персональных данных. С учетом особой чувствительности сферы для обеспечения гарантий прав субъектов персональных данных такие изъятия должны предполагать повышенную защиту персональных данных.

4. Совершенствование режима экспорта систем искусственного интеллекта и робототехники

В целях развития российских разработок технологий искусственного интеллекта и робототехники необходимо сформировать благоприятный режим их экспорта. Меры, ограничивающие экспорт, должны применяться только в сферах, непосредственно затрагивающих интересы национальной безопасности.

Необходимо избегать формирования «двойного контура» регулирования, при котором российские разработчики будут вынуждены осуществлять инвестиции в разработку таких продуктов отдельно для российского рынка и международных рынков.

В частности, существующее регулирование содержит изъятия из списка товаров и технологий двойного назначения, которые могут быть использованы при создании вооружений и военной техники и в отношении которых осуществляется экспортный контроль в части продуктов с применением искусственного интеллекта и робототехники. Такой перечень изъятий для гражданского назначения является не в полной мере актуальным. Целесообразно расширить этот перечень либо перейти к описанию конкретных технологических решений и продуктов искусственного интеллекта и робототехники, экспорт которых может привести к их использованию при создании вооружений и военной техники.

5. Развитие страховых институтов

В настоящее время существует неопределенность в возможности применения существующих страховых институтов к отношениям с участием систем искусственного интеллекта и робототехники. Отсутствие специальных положений на этот счет делает невозможным страхование систем искусственного интеллекта и робототехники (что негативно сказывается на возможности их внедрения) либо делает его необоснованно дорогим (что также препятствует развитию отрасли).

Эффективное функционирование страховых институтов в индустрии, напротив, оказывает положительное влияние на скорость внедрения роботов в гражданский оборот. Так, наличие заключённого договора страхования ответственности за причинение вреда может выступать (и в целом ряде зарубежных стран выступает) ключевым условием для выпуска некоторых видов систем искусственного интеллекта и робототехники в оборот.

В связи с этим следует определить случаи и условия обязательного страхования ответственности за вред, причиненный применением роботов или систем искусственного интеллекта и робототехники, в том числе как альтернативы иным инструментам регулирования.

Определение случаев и условий применения страхования возможно после формирования нормативно-правовой и нормативно-технической базы в сфере искусственного интеллекта и робототехники, что позволит определить условия осуществления страхования, включая вопросы сбора статистических данных для расчета страховых тарифов, а также форму страхования (обязательное или добровольное).

6. Разработка и уточнение терминов и определений в сферетехнологий искусственного интеллекта и робототехники

Отсутствие однозначного понимания содержания терминов «искусственный интеллект», «робот», «умный робот», «робототехника», «интеллектуальный агент» приводит к терминологическим проблемам при формировании регулирования.

В то же время с учетом прикладного характера применения этих технологий в самых разных областях может требоваться формулирование разных определений в зависимости от отрасли применения технологий искусственного интеллекта и робототехники. По этой причине в

рассматриваемый в Концепции временной период предлагается по возможности избегать внедрения в законодательство Российской Федерации единого для всех отраслей нормативного определения указанных терминов. При этом крайне важно в этот период провести работу по построению и гармонизации онтологии предметной области силами экспертного сообщества и профильных технических комитетов при Федеральном агентстве по техническому регулированию и метрологии. Там, где это необходимо для целей определения предмета регулирования конкретных нормативных правовых актов, предлагается использовать определения, содержащиеся в документах по стандартизации, либо давать определения, актуальные конкретно для этой сферы регулирования.

7. Обеспечение безопасности, в том числе информационной

Обеспечение необходимого уровня безопасности систем искусственного интеллекта и робототехники является ключевым условием внедрения таких технологий. Законодательство Российской Федерации, как правило, уже содержит общие требования к безопасности продуктов (в том числе товаров, работ и услуг), однако с учетом развития технологий искусственного интеллекта и робототехники эти требования в ряде случаев должны быть уточнены.

Так, для отдельных категорий роботов или систем искусственного интеллекта в зависимости от степени риска их использования могут быть установлены нормативными правовыми актами, стандартами и документами саморегулируемых и иных организаций специфические требования безопасности.

Развитие правового регулирования в сфере обеспечения информационной безопасности должно происходить с учетом целей, задач и содержания законодательства Российской Федерации об информационной безопасности, включая правовое регулирование развития критической информационной инфраструктуры и защиту персональных данных граждан Российской Федерации.

8. Разработка нормативных правовых актов в сфере искусственного интеллекта и робототехники на международном уровне

Международные организации и межгосударственные объединения различного характера ведут обсуждения инициатив в рассматриваемой сфере или уже реализуют их.

Необходимо обеспечить учёт национальных интересов Российской Федерации, её граждан и представителей отечественных компаний при формировании международного регулирования в этой сфере, а также интегрировать Российскую Федерацию в международный рынок искусственного интеллекта и робототехники с точки зрения универсальности правового регулирования и использования базовых международных принципов. Это предполагает активное вовлечение представителей Российской Федерации в разработку международных документов в сфере искусственного интеллекта и робототехники, прежде всего в Организации экономического сотрудничества и развития, Совете Европы, Организации Объединенных Наций и её специализированных учреждениях.

9. Создание нормативных условий для применения систем искусственного интеллекта при принятии юридически значимых решений

Требуются выявление и анализ сфер, в которых допускается ограниченное применение систем искусственного интеллекта при принятии юридически значимых решений, составление перечня таких сфер, подготовка предложений о корректировке соответствующих нормативных правовых актов. При этом по меньшей мере в рассматриваемый в Концепции временной период законодательство Российской Федерации должно допускать только точечное «делегирование» определенных решений системам искусственного интеллекта, где это объективно целесообразно и не несет угрозы основополагающим правам и свободам человека, обороне страны и безопасности государства. Для реализации отдельных элементов «делегирования» может активно применяться инструмент экспериментальных правовых режимов («регуляторные песочницы»).

10. Предложение систем искусственного интеллекта и робототехники в качестве товара (работы, услуги), обеспечивающего удовлетворение личных и семейных нужд потребителей

Применение систем искусственного интеллекта и робототехники как более функциональных по сравнению с традиционными системами потенциально способно повысить качество жизни потребителей.

В то же время не всегда понятная и предсказуемая логика работы таких систем создает ряд рисков для потребителей, например, при применении систем искусственного интеллекта и робототехники, предназначенных для автоматизации совершения сделок и иных юридических действий, а также при применении систем искусственного интеллекта и робототехники, взаимодействующих с физической средой (бытовые роботы, электроника, системы «умного дома» и др.).

Вместе с тем в рассматриваемый в Концепции период внесение в законодательство Российской Федерации каких-либо дополнительных ограничений на применение таких систем представляется нецелесообразным.

Также применение всех типов подобных систем ввиду повышения интенсивности обработки персональных данных сопряжено с дополнительными рисками нарушения тайны частной жизни граждан.

С учетом изложенного целесообразно:

- уточнить там, где это необходимо с учетом специфики товара (работы, услуги), подход к подтверждению и оценке соответствия продукции при внедрении в нее систем искусственного интеллекта и робототехники с учетом их особенностей (изменение поведения в процессе эксплуатации), включая оценку соответствия функциональным требованиям и требованиям безопасности;

- уточнить необходимость и возможные случаи введения в системы искусственного интеллекта и робототехники, которые потенциально могут причинить вред, функциональных особенностей, обеспечивающих, например, возможность потребителя прекратить деятельность системы искусственного интеллекта в критической ситуации («красная кнопка») и (или) обеспечить фиксацию фактов, позволяющих установить обстоятельства причинения вреда («черный ящик»);

- стимулировать выработку и закрепление разработчиками и производителями соответствующих систем этических норм в области обработки информации (включая персональные данные), добросовестного

информирования об основных функциональных особенностях систем искусственного интеллекта и робототехники, а также внедрение систем добровольной сертификации соответствия таким нормам;

- уточнить порядок реализации существующих прав потребителей с учетом особенностей товаров (работ, услуг), функциональность которых определяется и может изменяться программным обеспечением.

11. Совершенствование системы технического регулированияи оценки соответствия

В настоящее время в Российской Федерации действует целый ряд технических стандартов в сфере робототехники, однако нормативно-техническое регулирование в области искусственного интеллекта только начинает формироваться.

Для обеспечения надежности, достоверности, безопасности и интероперабельности решений в области искусственного интеллекта необходимо создание современной системы нормативно-технического регулирования в этой сфере.

Для отдельных сфер применения систем искусственного интеллекта и робототехники могут быть адаптированы существующие, а в некоторых случаях введены новые процедуры добровольного подтверждения соответствия, учитывающие достигнутый и перспективный уровень техники, роль программного компонента в функциональности и безопасности таких систем, особенности современных подходов к разработке программного обеспечения, его обновлению и сопровождению на протяжении жизненного цикла.

Установление в исключительных случаях требований обязательного подтверждения соответствия должно способствовать развитию оборота продуктов на основе искусственного интеллекта и робототехники, выступая достаточным условием их введения в оборот и (или) альтернативой иных регуляторных ограничений, связанных с обеспечением безопасности отдельных видов продуктов на основе технологий искусственного интеллекта и робототехники. При этом не может допускаться установление требований обязательного подтверждения соответствия до разработки соответствующих стандартов или иных требований.

В тех случаях, когда это возможно, вместо требований обязательного подтверждения соответствия должны использоваться меры, ограничивающие в меньшей степени развитие отрасли.

Целесообразно обеспечить активное участие российских специалистов в разработке международных стандартов и иных документов, в том числе на международных ключевых площадках (Международная организация по стандартизации, Международная электротехническая комиссия, Международный союз электросвязи, Организация экономического сотрудничества и развития, Институт инженеров электротехники и электроники).

12. Совершенствование порядка охраны прав на результаты интеллектуальной деятельности

Существующий правовой режим не обеспечивает правовую охрану результатов деятельности систем искусственного интеллекта, полученных без творческого вклада человека. Потенциальная «неохраноспособность» результатов деятельности, полученных с использованием систем искусственного интеллекта и робототехники, может дестимулировать разработку и внедрение таких систем.

Необходимо выработать подходы к наиболее спорным вопросам.

В частности, необходимо определить:

- целесообразно ли расширить толкование понятия творческого вклада и (или) предоставить правовую охрану таким результатам как объектам интеллектуальной собственности в другом формате. Если целесообразно, кто должен быть субъектом, обладающим исключительным правом на результат интеллектуальной деятельности, в каком режиме и с какими возможными изъятиями должна быть предоставлена правовая охрана таким результатам интеллектуальной деятельности;

- при каких условиях допустимо использование при разработке и эксплуатации систем искусственного интеллекта и робототехники (в частности, при машинном обучении) результатов интеллектуальной деятельности третьих лиц.

Другим аспектом проблемы является необходимость совершенствования порядка закрепления прав на результаты интеллектуальной деятельности, созданные с использованием технологий искусственного интеллекта и робототехники.

13. Иные общеотраслевые задачи регулирования применения технологий искусственного интеллекта и робототехники

Для привлечения иностранных специалистов высокого уровня в сфере искусственного интеллекта и робототехники необходимо предусматривать меры, облегчающие их въезд в Российскую Федерацию и работу на ее территории.

Целесообразно включение программ повышения цифровой грамотности в общеобразовательные программы (в целях повышения доверия к технологиям искусственного интеллекта и робототехники со стороны общества).

При выработке государственной политики в сфере занятости необходимо учитывать влияние, которое может оказать расширение применения систем искусственного интеллекта и робототехники на рынок труда и на востребованность отдельных профессий.

Для внедрения образовательных программ в сфере искусственного интеллекта и робототехники необходимо проработать вопрос уточнения правил лицензирования образовательной деятельности по образовательным программам с использованием дистанционных образовательных технологий, создания новых (экспериментальных) образовательных программ.

III. Отраслевые направления совершенствования регулирования применения технологий искусственного интеллекта и робототехники

1. Законодательство Российской Федерации в сфере охраны здоровья граждан

На основе технологий искусственного интеллекта разрабатываются системы диагностики и поддержки принятия врачебных решений, которые позволяют использовать массивы аналитической информации, недоступные или ограниченно доступные медицинским работникам при обычном взаимодействии с пациентом.

В свою очередь, использование оцифрованных массивов медицинских данных разработчиками для обучения систем искусственного интеллекта и робототехники способно значительно повысить эффективность и безопасность таких систем.

Медицинская робототехника является одним из самых быстро растущих сегментов робототехники и обеспечивает оказание более качественных услуг пациентам.

Ключевыми барьерами существующего регулирования, препятствующими широкому использованию технологий искусственного интеллекта и робототехники в медицине и требующими правового решения, в том числе посредством широкого применения экспериментальных правовых режимов, являются:

- проблема распределения ответственности за вред здоровью пациента, наступивший в результате применения технологий искусственного интеллекта и робототехники в процессе оказания медицинской помощи, вследствие отсутствия законодательно установленного перечня случаев, при которых допускается полное или частичное принятие решений с применением систем искусственного интеллекта и робототехники;

- неопределённость в вопросах отнесения систем искусственного интеллекта и робототехники (включая приложения, чат-боты и др.) к медицинским изделиям, подлежащим государственной регистрации;

- отсутствие специального порядка регистрации систем искусственного интеллекта и робототехники и медицинских роботов, учитывающего их специфику, а также долгие сроки прохождения соответствующих процедур, которые не позволяют быстро выводить на рынок новые решения, оперативно вносить изменения в системы искусственного интеллекта и робототехники и пользовательскую документацию в связи с необходимостью регулярных обновлений программного обеспечения;

- низкая доступность медицинских данных в целом и качественных размеченных данных в особенности для использования разработчиками систем искусственного интеллекта и робототехники в связи с отсутствием достаточных правовых оснований для предоставления права использования обезличенных медицинских данных третьим лицам, регламентов передачи медицинских данных от медицинских организаций компаниям – разработчикам систем искусственного интеллекта и робототехники.

2. Нормативно-правовое регулирование использования технологий искусственного интеллекта и робототехники в государственном (муниципальном) управлении

Использование технологий искусственного интеллекта и робототехники в государственном (муниципальном) управлении потенциально позволит сократить количество рутинных операций у государственных (муниципальных) служащих, минимизировать издержки и повысить скорость принятия решений.

Внедрение технологий искусственного интеллекта и робототехники в рассматриваемой сфере целесообразно осуществлять поэтапно, начиная со сфер применения, которые не предполагают принятия критически значимых решений.

Ключевые проблемы существующего регулирования использования систем искусственного интеллекта и робототехники в государственном (муниципальном) управлении заключаются в отсутствии однозначного понимания нормативных условий для использования систем искусственного интеллекта и робототехники при принятии каких-либо юридически значимых решений, в том числе в части:

- рассмотрения обращений граждан;
- предоставления государственных (муниципальных) услуг;
- осуществления действий разрешительного характера;
- осуществления контрольно-надзорных мероприятий.
- Для решения этих проблем требуется:
- повышение качества данных в государственных и муниципальных информационных системах, в том числе за счет создания национальной и региональных систем управления данными;
- создание нормативных возможностей применения систем искусственного интеллекта и робототехники для принятия определенных решений в сфере государственного управления;
- создание механизма пересмотра решений, принятых с помощью систем искусственного интеллекта;
- утверждение прозрачных правил оценки соответствия систем искусственного интеллекта и робототехники требованиям безопасности, выработка механизма оценки эффекта от их применения с точки зрения защиты основополагающих прав человека и гражданина (защита от

дискриминации и избирательного правоприменения, сокращение рисков разглашения конфиденциальной информации и др.).

3. Законодательство Российской Федерации в сфере транспорта

Технологии искусственного интеллекта и робототехники активно применяются для создания и эксплуатации высоко- и полностью автоматизированного транспорта (автомобильного, рельсового, воздушного, водного). Применение технологий автоматического управления позволяет сделать транспорт более безопасным, экономичным, быстрым и комфортным.

Несмотря на развитие технологий автоматического управления во всех видах транспорта, отраслевое транспортное законодательство Российской Федерации, как правило, не допускает либо серьезно ограничивает возможности эксплуатации транспортных средств с применением автоматических систем без участия человека.

Для эффективного развития различных видов транспорта с применением систем искусственного интеллекта и робототехники требуется реализация ряда нормативных мероприятий.

В сфере автомобильного транспорта ключевая сложность в развитии «беспилотных» автомобилей связана со сложной процедурой допуска высокоавтоматизированных транспортных средств на дороги общего пользования и отсутствием регламентированного порядка допуска высокоавтоматизированных транспортных средств 4 и 5 уровня автоматизации по стандартам Международной ассоциации автомобильных инженеров (SAE).

Также требуется уточнить порядок опытной эксплуатации высокоавтоматизированных транспортных средств, в том числе скорректировать минимальные характеристики безопасности испытательных образцов высокоавтоматизированных транспортных средств для опытной эксплуатации на дорогах общего пользования, отменить избыточные сертификационные испытания, регламентировать порядок допуска испытательных образцов высокоавтоматизированных транспортных средств без участия водителя с удаленным доступом оператора к высокоавтоматизированным транспортным средствам или с водителем на пассажирском месте (не принимающим активного участия в управлении транспортным средством). Требуется определить порядок регламентации коммерческой эксплуатации высокоавтоматизированных транспортных средств и порядок определения ответственности в случае нанесения вреда со стороны высокоавтоматизированных транспортных средств.

В сфере воздушного транспорта целесообразно совершенствование регулирования использования беспилотных воздушных судов, в том числе уточнение порядка регистрации, учета и использования беспилотных воздушных судов, упрощение порядка получения и использования данных с помощью беспилотных воздушных судов, в том числе при проведении картографической съемки. При этом необходима разработка схем воздушного движения, ориентированных на массовое использование беспилотных воздушных судов в качестве транспортных средств.

В сфере железнодорожного транспорта требуется создание нормативных возможностей функционирования систем автоматического или дистанционного управления тяговым подвижным составом, установление требований к автоматическому управлению маневровым локомотивом без машиниста, установление правил управления тормозами железнодорожного подвижного состава в автоматическом и дистанционном режимах.

В сфере водного транспорта требуется совершенствование законодательства для развития безэкипажного судовождения, порядка выпуска в обращение и эксплуатации морской и речной техники с высокой степенью автоматизации управления.

Отдельно следует проработать вопрос о снятии ограничений при использовании самоходной техники специального назначения (сельскохозяйственная техника, производственный транспорт, коммунальные машины). В частности, в настоящее время отсутствует нормативная база, прямо регламентирующая движение автономного транспорта на закрытых территориях производственных предприятий.

Необходимо создать правовые нормы, позволяющие перейти от использования высокоавтоматизированного транспорта исключительно в режиме эксперимента к возможности его использования на постоянной основе.

4. Законодательство Российской Федерации о градостроительной деятельности

Формирование сведений о здании, установленном оборудовании, эксплуатационных режимах, рисках и ответственности эксплуатирующей организации за нештатные ситуации, а также оценка безопасности строительства и эксплуатации зданий и объектов инфраструктуры могут осуществляться с применением технологий искусственного интеллекта и робототехники.

Также технологии искусственного интеллекта и робототехники могут применяться для построения эффективных систем внутренней логистики зданий, в том числе с применением беспилотных и сервисных роботов.

Законодательство Российской Федерации о градостроительной деятельности не в полной мере обеспечивает благоприятные условия для формирования и сбора данных, достаточных для предиктивной аналитики условий эксплуатации зданий и сооружений, а также повторного использования указанных данных при разработке проектов новых объектов, что требует уточнения.

Контрольно-надзорная деятельность по обеспечению безопасности эксплуатации зданий также построена на традиционных методах контроля.

Целесообразно предусмотреть в законодательстве Российской Федерации возможность осуществления дистанционного государственного контроля (надзора) (в случае заинтересованности хозяйствующих субъектов в осуществлении государственного контроля (надзора) в такой форме).

5. Использование систем искусственного интеллекта и робототехники для реализации концепции «умного города»

В этих целях необходимо определить и снять регуляторные барьеры, в том числе препятствующие:

- автоматизации жилищно-коммунального хозяйства и коммунальных услуг (учет показаний счетчиков и осуществление «гибкой» подачи ресурсов в зависимости от переменных показателей, автоматическое определение уровня шума, загрязнения и его анализ, контроль работы оборудования и др.);

- внедрению «умного» городского транспорта (в части развития «беспилотного» транспорта и развития сопровождающей его инфраструктуры – систем фото- и видеофиксации правонарушений, систем автоматического администрирования городского парковочного пространства, систем автоматического управления транспортными потоками в зависимости от загруженности проезжей части, систем автоматического контроля за состоянием дорожного полотна и дорожно-транспортной инфраструктуры, систем составления маршрутов общественного транспорта на основе анализа больших данных и др.);

- созданию цифровых платформ и сервисов для вовлечения горожан в управление городскими процессами (введение голосования по конкретным

вопросам, анализ с помощью систем искусственного интеллекта текстуальных обращений для выявления общего отношения к проблеме или самих проблем, анализ выраженного общественного мнения);

- внедрению интеллектуальных систем общественной безопасности (систем видеонаблюдения с функциями биометрической идентификации и др.);
- генеральному планированию и планированию развития территорий на основе искусственного интеллекта и обрабатываемых им больших данных.

При этом особое внимание должно быть уделено пересмотру подхода к обязательному участию человека в принятии решений в обозначенных сферах (от необходимости участия человека в совершении конкретного действия к оперативному и стратегическому целеполаганию и контролю со стороны человека).

6. Законодательство Российской Федерации в финансовой сфере

В финансовом секторе технологии искусственного интеллекта имеют широкие возможности для применения. Это использование технологий искусственного интеллекта для осуществления алгоритмической торговли («торговые роботы»), применение технологий искусственного интеллекта кредитными организациями для клиентского обслуживания и для осуществления деятельности, напрямую не связанной с обслуживанием клиентов, обработка различного рода финансовых данных, в том числе большого массива данных о банковских операциях, анализа рынков и рыночной информации, финансовой отчетности. Каждая сфера применения технологий искусственного интеллекта в финансовом секторе предполагает специфическое регулирование в зависимости от конкретных условий их внедрения.

Соблюдение баланса между внедрением новых технологий и соблюдением прав граждан и интересов государства на крайне чувствительных к регуляторному воздействию финансовых рынках должно предполагать использование самых гибких инструментов.

Ключевым из них является создание экспериментальных правовых условий применения отдельных новых инструментов (экспериментальные правовые режимы). Широкое использование этих механизмов для апробации новых финансовых сервисов и технологий в сфере искусственного интеллекта (там, где объективно требуется воздействие регулятора) должно выступать в качестве целевого состояния регулирования в финансовой сфере.

Возможное установление дополнительных ограничительных условий (например, условий осуществления обработки данных в финансовом секторе, отличных от общего регулирования, особых условий распределения ответственности игроков финансового рынка при применении систем искусственного интеллекта, определения требований к использованию экспертных систем искусственного интеллекта для принятия отдельных решений) предлагается реализовывать только после комплексной оценки их регулирующего воздействия, в том числе за счет тестирования условий применения технологий искусственного интеллекта в финансовом секторе в режиме экспериментального правового режима («регуляторной песочницы»). Там, где это возможно, следует стремиться использовать инструменты саморегулирования и сорегулирования, прежде всего стандарты саморегулируемых организаций.

7. Законодательство Российской Федерации в области космической деятельности

В космической деятельности технологии робототехники изначально очень активно применяются, благодаря чему в отрасли существуют технологии, имеющие высокий коммерческий потенциал в гражданском обороте.

Однако регулирование порядка использования компонентов робототехники в гражданских целях затрудняет их развитие в этом направлении.

С учетом высокой перспективности сферы космической деятельности для развития технологий искусственного интеллекта и робототехники важно уточнить регуляторные механизмы в указанной сфере.

Для этого необходимы совершенствование законодательства Российской Федерации для целей использования разработок космической промышленности в гражданском назначении, проработка регуляторных механизмов развития частной космонавтики и совершенствования институтов государственно-частного партнерства, анализ вариантов упрощения порядка использования технологий искусственного интеллекта и робототехники в космонавтике.

8. Законодательство Российской Федерациив сфере промышленности

В промышленности технологии искусственного интеллекта и робототехники помогают значительно повысить эффективность предприятий в машиностроении, металлургии, горной добыче, нефтегазовом секторе, химической промышленности и других отраслях.

Опытная эксплуатация систем искусственного интеллекта и робототехники на предприятиях топливно-энергетического комплекса требует создания специальных полигонов общего доступа. Необходимо оценить и при необходимости устранить возможные необоснованные регуляторные ограничения, препятствующие эффективному применению таких полигонов.

Реализации потенциала искусственного интеллекта и робототехники препятствует ряд барьеров, многие из которых являются смежными (например, проблема использования наземной и воздушной беспилотной техники).

Кроме того, требует проработки вопрос о снятии барьеров, связанных с ограничением сбора и обработки информации о промышленном оборудовании для системной обработки и создания систем искусственного интеллекта. Схожие барьеры связаны с использованием данных в промышленности. Существуют вопросы безопасной передачи промышленных данных, возникновения прав на них, публикации отдельных видов промышленных данных и др.

9. Иные отраслевые направления совершенствования применения технологий искусственного интеллекта и робототехники

Технологии искусственного интеллекта и робототехники повсеместно внедряются в различных отраслях экономики. Это приводит к возникновению большого числа неочевидных локальных регуляторных проблем, актуальных для конкретной сферы либо конкретной разновидности систем искусственного интеллекта и робототехники.

Ключевыми задачами развития законодательства Российской Федерации в различных сферах являются следующие:

- создание механизма оперативного выявления локальных отраслевых регуляторных барьеров;
- разработка механизма координации полномочий органов государственной власти в случае «пересечения» их полномочий. Одним из

перспективных решений этой проблемы может стать выделение в государственном управлении самостоятельной функции по выработке и реализации государственной политики в сфере технологий искусственного интеллекта и робототехники;

- создание механизма быстрого снятия возникающих отраслевых барьеров, например, за счет внедрения режима экспериментального регулирования, локальной «регуляторной гильотины».

IV. Регуляторные меры для финансового стимулирования развития отрасли

В настоящее время в Российской Федерации уже предусмотрен ряд мер поддержки компаний, специализирующихся на разработке технологий искусственного интеллекта и робототехники. Вместе с тем такие меры поддержки фрагментарны и сложны в администрировании, информация о возможности и порядке их применения не всегда доводится до заинтересованных лиц системным образом. Необходимо оценить целесообразность и по итогам такой оценки проработать дополнительные меры поддержки по трем направлениям: стимулирование предложения, стимулирование спроса, развитие государственно-частного партнерства.

Применительно к поддержке развития государственно-частных партнерств следует проанализировать и реализовать дополнительные исследования относительно потенциала и эффекта использования такой меры, а также усовершенствовать законодательство в целях расширения возможностей для создания профильных государственно-частных партнерств, в том числе в отдельных сферах применения этих технологий (включая медицину, космонавтику, транспорт и др.), например в направлении технологических консорциумов.

V. Механизмы реализации Концепции

Реализация Концепции осуществляется следующими способами:

в качестве целевого ориентира при подготовке нормативных правовых актов и документов стратегического планирования в различных сферах (концепций, стратегий, «дорожных карт» и др.);

При изменении и планировании новых мероприятий федеральных проектов «Нормативное регулирование цифровой среды», «Цифровые технологии» и иных федеральных проектов национальной программы «Цифровая экономика Российской Федерации» и (или) посредством формирования плана принятия нормативных правовых актов, определяющего перечень первоочередных изменений в законодательство Российской Федерации для целей развития искусственного интеллекта и робототехники на основе принципов, подходов и предложений, предусмотренных Концепцией.

В предметной работе по реализации Концепции должны совместно участвовать представители органов государственной власти, отрасли, бизнес-ассоциаций, соответствующих институтов развития, общественных, научных и образовательных организаций.

При этом для выработки положений нормативных правовых актов, сбалансированных с точки зрения интересов экономики, общества и государства, в целях аналитической поддержки на всех этапах реализации Концепции следует запланировать проведение междисциплинарных и межотраслевых научных исследований, включая исследование международного опыта.

Следствием реализации Концепции должны стать разработка и принятие к 2024 году нормативных правовых актов в сфере искусственного интеллекта и робототехники, создающих комфортную регуляторную среду для развития технологий искусственного интеллекта и робототехники, в том числе по следующим направлениям:

- расширение регуляторных мер для финансового стимулирования развития технологий искусственного интеллекта и робототехники;
- создание механизмов упрощенного внедрения технологий искусственного интеллекта и робототехники;
- решение общеотраслевых задач развития законодательства Российской Федерации, включая обеспечение безопасности систем искусственного интеллекта и робототехники;
- снятие отраслевых барьеров для внедрения технологий искусственного интеллекта и робототехники;
- совершенствование режима оборота данных для целей развития искусственного интеллекта и робототехники;
- совершенствование системы технического регулирования в сферах искусственного интеллекта и робототехники;

- участие в разработке актов в сфере искусственного интеллекта и робототехники на международном уровне.

Уточнение способов реализации Концепции должно осуществляться с учетом результатов мониторинга ее реализации и динамики развития технологий искусственного интеллекта и робототехники в Российской Федерации и в мире.





На пути к инновациям в области ИИ

Второй доклад об искусственном интеллекте для правоохранительных органов

Правовая оговорка

Мнения, выводы, заключения и рекомендации, изложенные в настоящем документе, необязательно отражают точку зрения Интерпола, ЮНИКРИ или любого другого соответствующего национального, регионального или международного органа. Используемые обозначения и материалы, представленные в настоящей публикации, не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединённых Наций относительно правового статуса какой-либо страны, территории,

города или района её властей или относительно делимитации её границ. Содержание настоящей публикации может цитироваться или воспроизводиться при условии упоминания источника информации. ЮНИКРИ и Интерпол хотели бы получить копию документа, в котором эта публикация используется или цитируется.

Выражение признательности

Настоящий доклад подготовлен совместно ЮНИКРИ и Интерполом. Он был подготовлен Одраном Маккарти и Марией Эйрой (ЮНИКРИ) при поддержке Софи ван де Меуленграаф, Джейка Келли (ЮНИКРИ) и Кевина Джоэла Энтони (Интерпол) и под руководством Ираклия Беридзе (ЮНИКРИ) и Штеффена Усдала (Интерпол).

Интерпол и ЮНИКРИ хотели бы выразить свою признательность экспертам и должностным лицам за участие во втором глобальном совещании по ИИ для правоохранительных органов, состоявшемся в Сингапуре в июле 2019 года, и отметить вклад всех тех, кто поддержал организацию этого совещания и рассмотрение настоящего доклада.

Предисловие

Преступность не стоит на месте, она динамична, постоянно развивается и постоянно адаптируется к новым реалиям, становясь все более сложной и порождает множество новых проблем. За последние два столетия мы стали свидетелями того, как на первый план выходят новые виды преступлений, а традиционные преступления принимают различные формы или вообще приобретают совершенно новый облик. До тех пор, пока преступления и преступность сохраняют динамичный характер, правоохранительные органы должны быть готовы идти в ногу со временем и гибко адаптироваться к растущим тенденциям и событиям, чтобы обеспечить безопасность общества. Искусственный интеллект (далее ИИ) может быть козырем, чтобы это реализовать. Способность ИИ изменять саму природу полицейской деятельности и повышать эффективность и результативность, например, выявлять из толпы лиц, представляющих интерес; прогнозировать и предсказывать насилие; автоматически сортировать, помечать и классифицировать большой объём оперативных данных, таких как улики или

запрещённые материалы; и даже отслеживать факторы, способствующие радикализации, в начале их проявления.

Мы стремились сформировать этот доклад, придать ему смысл и цель, а также позиционировать его как глобальную платформу для сотрудничества и взаимодействия правоохранительных органов в области ИИ

Настоящий доклад об ИИ для правоохранительных органов является самым последним результатом сотрудничества между Инновационным центром международной организации уголовной полиции (Интерпол) и центром ИИ и робототехники межрегионального научно-исследовательского института Организации Объединённых Наций по вопросам преступности и правосудия (ЮНИКРИ). Вместе мы создали уникальный форум для правоохранительных органов, чтобы обсудить достижения в области ИИ, а также последствия использования этой технологии для борьбы с преступностью. С тех пор как мы начали нашу работу в начале 2018 года, мы стремились придать ей смысл и цель, а также позиционировать её как глобальную платформу для сотрудничества и взаимодействия Правоохранительных органов в области ИИ. Мы имели честь и привилегию провести второе глобальное совещание Интерпол – ЮНИКРИ по ИИ для правоохранительных органов в рамках Всемирного форума.

Интерпол – передовой мировой форум по изучению инноваций для правоохранительных органов. Идёт подготовка к третьему ежегодному глобальному совещанию Интерпол – ЮНИКРИ по ИИ для правоохранительных органов в Гааге, Нидерланды, в ноябре 2020 года. Растущий интерес и внимание, которые получают эти встречи, являются одновременно наградой для Интерпола и ЮНИКРИ и свидетельствуют о растущей значимости ИИ для сообщества уголовного правосудия.

Законность, общественное признание, надёжность, ответственность и этика – важные понятия, которые читатели с полным основанием будут регулярно повторять на протяжении всего настоящего доклада. Действительно, несмотря на большой потенциал ИИ, использование этой технологии правоохранительными органами также вызывает очень реальные и серьёзные опасения в области прав человека, которые могут нанести огромный ущерб и подорвать доверие, оказываемое обществом правоохранительным органам.

Права человека, гражданские свободы и даже основополагающие принципы права, на которых зиждется наша система уголовного правосудия, могут оказаться неприемлемо уязвимыми или даже непоправимо скомпрометированными, если мы не пойдём по этому пути с крайней осторожностью.

Суматоха, вызванная появлением нового коронавируса SARS-CoV-2 в конце 2019 года и продолжающейся пандемией COVID-19, вызванная этим вирусом, подчёркивает важность этого. Поскольку мировое правоохранительное сообщество оказывается в центре беспрецедентной ситуации, играя решающую роль в пресечении распространения вируса, сохранении общественной безопасности, социального порядка, новые технологии, такие как ИИ, станут мощным ресурсом в борьбе с преступностью. Однако даже в кризисные времена мы должны стремиться отстаивать основополагающие принципы права и обеспечивать уважение верховенства закона.

По этим причинам мы считаем необходимым чётко и с самого начала подчеркнуть, что ничто в настоящем докладе не должно восприниматься ни Интерполом, ни ЮНИКРИ как одобрение какого-либо конкретного случая использования ИИ для правоохранительных органов на данном этапе.

На самом деле, мы находим большое утешение в прогрессивных, открытых и серьёзных дискуссиях, которые мы провели на втором глобальном совещании прошлым летом, именно по этой критической двойственности ИИ, которая нуждается в дальнейшем понимании и развитии. Мы приветствуем выявление необходимости специального руководства и поддержки со стороны правоохранительных органов для содействия внедрению ИИ и тем самым избежания не только «возможных», но и «неизбежных» провокаций при его использовании.

Благодаря тесному сотрудничеству между Интерполом и ЮНИКРИ мы надеемся, в конечном счёте, внести свой вклад в восполнение этого пробела, оказывая поддержку в выявлении текущих и потенциальных случаев использования и предоставляя указания по разработке, развёртыванию и использованию систем ИИ в правоохранительных органах, как законным, так и заслуживающим доверия образом. Эта поддержка и указания начинаются с настоящего доклада, в котором содержатся ключевые выводы из обсуждений на втором глобальном совещании, дополненные дальнейшим экспертным анализом и последними событиями.

Они будут продолжены на третьем глобальном совещании в Гааге. Поэтому вопрос, который мы должны задать, заключается не в том, должны ли правоохранительные органы использовать ИИ, а в том, как именно правоохранительные органы могут или должны использовать ИИ и как они делают это наиболее ответственным и надлежащим образом. Мы надеемся, что в настоящем докладе мы начнём отвечать на некоторые из этих вопросов.

Анита Хазенберг

Директор, Инновационный центр Интерпола

Ираклий Беридзе

Руководитель, Центр ЮНИКРИ по искусственному интеллекту и робототехнике





Основные положения

ИИ может стать мощным инструментом, позволяющим правоохранительным органам реализовать потенциал, изменяющий правила игры, повысить свою эффективность и расширить существующие возможности в борьбе со всеми формами преступности. Это также обоюдоострый меч, которым необходимо осторожно пользоваться, чтобы не нарушать основные права человека, такие как право на неприкосновенность частной жизни, равенство и недискриминацию.

Также нельзя подрывать основные принципы права, такие как презумпция невиновности, защита против самообвинения. Под эгидой инновационного центра Интерпола и ЮНИКРИ, через его центр искусственного интеллекта и робототехники, в июле 2019 года в Сингапуре состоялось второе глобальное совещание по ИИ для правоохранительных органов. В настоящем докладе отражены выступления и дискуссии, проведённые в ходе совещания, а также дополнен дальнейший анализ последних актуальных событий, касающихся использования ИИ в правоохранительных органах, включая текущие тенденции в областях ИИ и регулировании этой сферы. Он выходит за рамки простого отчёта о ходе разбирательства и вместо этого стремится служить практической ссылкой на

правоохранительные органы, которые намерены разрабатывать или развёртывать системы ИИ ответственным и эффективным образом. Она стремится оказать поддержку правоохранительным органам в деле лучшей концептуализации применения ИИ и дальнейшего углубления своего понимания концепций ответственного использования ИИ и предлагает ответственный путь развития системы для правоохранительных органов.

В первой главе описывается общий ландшафт использования ИИ в правоохранительных органах, в частности отмечается растущий интерес правоохранительного сообщества и подчёркивается необходимость сотрудничества между заинтересованными сторонами, с тем чтобы учиться друг у друга успехам и неудачам и быть в состоянии лучше смягчить любое вредное воздействие, вытекающее из использования этой технологии. В заключение глава подчёркивает, что правоохранительные органы должны также помнить о других угрозах, связанных с достижениями в области искусственного интеллекта, в частности о злонамеренном использовании его преступниками и террористическими группами.

Во второй главе описаны четыре основные области ИИ, рассматриваемые Интерполом и ЮНИКРИ, как имеющие отношение к правоохранительной деятельности, а именно: обработка звука, визуальная обработка, оптимизация ресурсов и обработка человеческой речи. Описаны некоторые возможные области применения в каждой из этих областей, а также практические и технические проблемы, которые необходимо учитывать правоохранительным органам при изучении этих областей применения для дальнейшей концептуализации потенциальных практических применений ИИ. Содействие обмену опытом и извлечённые уроки в третьей главе представлены в виде обзора ряда примеров использования ИИ, которые, разрабатываются или осуществляются национальными и местными правоохранительными органами в Австралии, Германии, Японии и Норвегии. Эти примеры использования были представлены соответствующими правоохранительными органами в ходе второго глобального совещания.

Признавая реальность того, что ИИ все больше интегрируется в правоохранительную деятельность, Глава 4 посвящена наиболее важному аспекту: ответственному использованию ИИ правоохранительными органами. Эта глава начинается с изложения общих принципов, которых должны стремиться придерживаться правоохранительные органы, а именно уважения прав человека, демократии, справедливости и верховенства закона, а также соответствующих требований справедливости, подотчётности, прозрачности и лёгкости восприятия, которые должны быть приняты для того, чтобы правоприменение соответствовало этим принципам. Кроме того, описываются конкретные правовые проблемы, соображения о важности социального

признания общественностью, а также последние этические рамки и заявления о принципах, разрабатываемые в Европе Организацией экономического сотрудничества и развития другими организациями.

В пятой главе начинается путь к осознанию ответственного использования ИИ в правоохранительных органах, а также определяются конкретные потребности полиции и рекомендации, представленные сотрудниками правоохранительных органов.

В главе шестой рассматривается предложение Интерпола и ЮНИКРИ о разработке оперативно ориентированного инструментария для оказания поддержки и руководства правоохранительным органам в области нормотворчества для внедрения ИИ. Описываются возможная цель, структура, целевая аудитория и ключевые моменты данного инструментария.

Доклад завершается седьмой главой, в которой определяются основные направления деятельности, которые должны быть рассмотрены международным правоохранительным сообществом, директивными органами и межправительственными организациями в целях поддержки разработки инструментария и дальнейшего развития и продвижения концепции ответственного ИИ для правоохранительных органов.

1. Интеграция ии в правоохранительных органах

Становится все более очевидным, что ИИ и связанная с ним экосистема новых и новейших технологий, от «Интернета вещей» до квантовых вычислений, могут оказывать глубокое влияние на общество. Это воздействие было подробно изучено с точки зрения правоохранительных органов на первом Глобальном совещании Интерпола – ЮНИКРИ по ИИ в 2018 году и представлено в докладе[1], опубликованном в 2019 году - ИИ для правоохранительных органов.

Второе глобальное совещание Интерпола – ЮНИКРИ по ИИ для правоохранительных органов состоялось в рамках Всемирной конференции Интерпола 2019 года – мероприятие, в котором приняли участие более 6000 человек и которое предоставило правоохранительным органам платформу для взаимодействия с партнёрами из деловых и академических кругов. Эта встреча дала толчок продуктивным дискуссиям и продемонстрировала, что значительный прогресс, инновации, исследования и разработки (НИОКР) были и остаются основополагающими.

[1] http://www.unicri.it/news/files/ARTIFICIAL_INTELLIGENCE_ROBOTICS_LAW%20ENFORCEMENT_WEB.pdf

Правоохранительное сообщество начало формировать чувство ответственности с точки зрения своих знаний и понимания тонкостей применения и интеграции ИИ. Правоохранительные органы все чаще изучают применение ИИ для удовлетворения конкретных потребностей или требований – так называемых «прецедентов использования». Некоторые из этих вариантов использования будут более подробно описаны ниже. Хотя на данный момент правоохранительные органы в значительной степени просто используют лишь основные инструменты ИИ –, использование истинных возможностей ИИ будет возможным в ближайшем и среднесрочном будущем. Технический прогресс, бесспорно, движется быстро и возможно, даже быстрее, чем правоохранительные органы могут адаптироваться и идти в ногу. Если правоохранительные органы действительно хотят извлечь выгоду из ИИ, они не могут сделать это в одиночку. Необходимость согласованных усилий по сотрудничеству в области ИИ для правоохранительных органов была подчёркнута на втором глобальном совещании в качестве одного из ключевых моментов для правоохранительных органов, чтобы воспользоваться возможностями, которые предоставляет ИИ.

Следующим важным шагом является налаживание сотрудничества в области искусственного интеллекта с заинтересованными сторонами в государственном секторе, промышленности, академических кругах, а также с соответствующими органами безопасности, разведывательными службами, органами по борьбе с терроризмом и так далее. Каждая заинтересованная сторона может как внести значительный вклад, так и извлечь выгоду из собственного уникального опыта правоохранительных органов. Опираясь на успехи друг друга и извлекая уроки из неудач, можно добиться значительного прогресса в разработке методов применения и интеграции ИИ. Цель правоохранительных органов должна заключаться не в создании параллельных программ НИОКР в области ИИ, а в расширении и поощрении обмена знаниями и технологиями, налаживании отношений и сотрудничестве между заинтересованными сторонами с тем, чтобы продвигать решения, которые требуются для практического применения.

В последнее время проявляется позитивный подход к сотрудничеству, при котором все чаще поощряется публикация и открытый обмен результатами исследований между правоохранителями. Одной из эффективных практик, обсуждавшихся в ходе второго глобального совещания, был набор студентов из университетов Национальной полицией Нидерландов для проведения конкретных научно-исследовательских мероприятий в пределах её территории и от лица полиции.

Правоохранительное сообщество начало формировать повышенное чувство зрелости с точки зрения своих знаний и понимания тонкостей применения и интеграции искусственного интеллекта.



Тем не менее взаимодействие с субъектами, не входящими в правоохранительные органы, не всегда бывает легким. Это может выявить проблемы конфиденциальности или безопасности, когда общая информация является личной, вредной, конфиденциальной или касается текущих расследований. Кроме того, практические проблемы возникают в тех случаях, когда сотрудничающие заинтересованные стороны используют различные подходы, практику или методы в области НИОКР.

Во время второго глобального совещания наряду с преимуществами были выделены некоторые практические проблемы сотрудничества с академическими кругами. Хотя быстрого решения этой проблемы не существует, одним из предлагаемых решений для преодоления практических различий в сотрудничестве с участием многих заинтересованных сторон была бы стандартизация систем, которая способствовала бы развитию технологий и косвенно активизации сотрудничества между секторами. В то время, как технологическая революция радикально меняет то, как работают люди, средства массовой информации, правительства, предприятия и политики, правоохранительные органы должны иметь в виду две перспективы: полезное использование и злонамеренное использование.

В своём вступительном слове на 73-й Генеральной Ассамблее Организации Объединённых Наций в 2018 году Генеральный секретарь ООН Антониу Гутерриш назвал риски, связанные с технологическим прогрессом2, одной из двух эпохальных проблем для человечества, отметив, что угрозы для бизнеса и государственных органов стали ещё более реальными.

По данным разработчика антивирусного программного обеспечения AVG, фишинг был самым распространенным методом доставки вредоносных программ в 2019 году и является причиной утечки 32% данных, остальные 68%

---

[2] Guterres, A. (2018, Sept 25). Address to the General Assembly. New York, UN Headquarters. Retrieved from https://www.un.org/sg/en/content/sg/speeches/2018-09-25/address-73rd-general-assemblv

инцидентов3 относятся к кибершпионажу. Подобные кибератаки могут быть использованы для мошенничества, вымогательства и шпионажа, они имеют разрушительные последствия. В то же время AVG также выявила рост числа вредоносных программ на базе ИИ в 2019 году, указывая на то, что киберпреступники уже используют автоматизированные инструменты для уклонения от обнаружения и замышляют новые атаки на модели ИИ, используя те же самые интеллектуальные технологии автоматизации, которые используют охранные компании для предотвращения вредоносных программ. Ещё одной растущей угрозой является злонамеренное использование небольших беспилотных летательных аппаратов (БПЛА) – широко известных как дроны. Хотя их использование в основном осуществляется с помощью ручного дистанционного управления и не в полной мере использует ИИ, развитие возможностей ИИ вскоре может привести к большей автономии. На сегодняшний день беспилотники используются с самодельными взрывными устройствами (СВУ) при атаках негосударственных субъектов в зонах конфликтов, таких как Сирия, Ирак или Украина4, а также для срыва операций в аэропортах, таких как аэропорт Гатвик в Соединённом Королевстве в декабре 2018 года5.

Возможно, самый большим прорыв, с точки зрения вредоносного использования ИИ, были достижения в программно генерируемых поддельных видео и изображениях, или так называемых «deepfakes».

В 2019 году мир стал свидетелем первого известного преступного использования этой технологии в Соединённом Королевстве6. Образ генерального директора энергетической компании был успешно сымитирован и использован для обмана партнёра, с целью перевода значительной суммы денег на личный счёт. Криминальный потенциал «deepfakes» огромен, как и возможность создания социальных и политических потрясений. В этой связи правоохранительные органы должны быть готовы не только использовать ИИ во благо, но и бороться с подобными угрозами сегодня и предвидеть будущие.

---

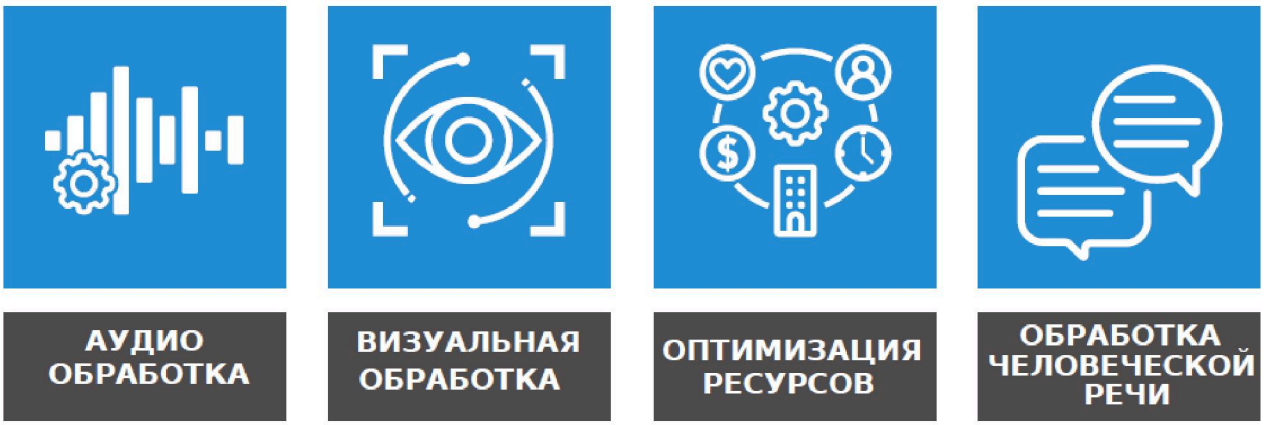
[3] AVG (2019, Dec 16). 20:20 Vision — 5 Threats to Watch Out for This Year. Retrieved from https://www.avg.com/en/signal/online-threats-in-2020

[4] to address the potential risks posed by terrorist use of unmanned aircraft systems. CTED Trends Alert. Retrieved from https://www.un.org/sc/ctc/wp-content/uploads/2019/05/CTED-UAS-Trends-Alert-Final_17_May_2019.pdf

[5] BBC News (2018, Dec 3). Gatwick Airport: Drones ground flights. Retrieved from https://www.bbc.com/news/uk-england- sussex-46623754

[6] Damiani, J. (2019, Sep 3). A Voice Deepfake Was Used To Scam A CEO Out Of $243,000. Forbes. Retrieved from https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/#af5474822416

2. Области искусственного интеллекта



Изучение окружающего мира – ценный ресурс

Он может помочь правоохранительным органам следить за последними технологическими достижениями и выявлять те из них, которые лучше всего подходят для того, чтобы внести свой вклад в их работу, восполнить пробелы в потенциале или расширить существующие возможности. В равной степени это ценный ресурс для политиков и лиц, принимающих решения в более широком сообществе уголовного правосудия, заключается в том, чтобы с юридической и этической точек зрения подготовить платформу для возможной интеграции таких технологий в правоохранительную деятельность.

В соответствии с этим и после проведения первого глобального совещания Интерпол и ЮНИКРИ провели предварительное сканирование горизонта области ИИ и определили четыре основные области, связанные с технологиями, основанными на ИИ, которые могут иметь самое непосредственное отношение к правоохранительным органам.

Для каждой из этих четырёх областей технологии ИИ были определены конкретные примеры использования, чтобы проиллюстрировать их актуальность и применение в правоохранительных органах. Далее следует краткий обзор каждой из этих четырёх областей ИИ и их применения в правоохранительных органах. Ниже приводится краткий обзор из каждой области технологии ИИ и выявленных вариантов её использования.

Следует отметить, что эти варианты использования не являются будущими возможностями, а являются реалиями сегодняшнего дня, которые разрабатываются и проверяются академическими и научными исследователями, а в некоторых случаях правоохранительными органами и органами безопасности.

Аудио обработка

Обработка звука – это манипулирование характеристиками аудиосигнала, например, для улучшения звука, отдельных источников, создания целых новых звуков, сжатия, хранения или передачи данных. Извлекая выгоду из достижений в таких научных областях, как лингвистика и анатомия, ИИ обещает полностью раскрыть потенциал обработки звука, что позволит ему осуществлять профилирование голоса с помощью ИИ.

Профилирование – это распространённый метод, используемый для экстраполяции релевантной информации из психологических и поведенческих характеристик индивида. В правоохранительных органах он часто используется в качестве инструмента расследования для поддержки идентификации возможных подозреваемых или увязки, казалось бы, разрозненных дел, которые могли быть совершены одним преступником. В дополнение к психологическим и поведенческим характеристикам, человеческий голос является ценным носителем, несущим с собой значительную личную информацию, которая, если её правильно расшифровать, может помочь в расследовании.

Уникальный голосовой отпечаток человека может быть законно собран правоохранительными органами с прослушиваемых телефонов, передаваемых по радио голосов, персональных интеллектуальных устройств или других устройств наблюдения. Приложения для профилирования голоса ИИ могут использовать такие голосовые отпечатки после того, как образцы разбиты на миллисекундные фрагменты. Исследуя этот голосовой отпечаток и анализируя, как звук вибрирует от и через уникальные физические структуры тела, система может вывести физические черты, такие как рост, вес, строение лица, возраст и даже сделать прогнозы относительно личности, физического здоровья и психического благополучия. Кроме того, информация о физической среде, окружающей говорящего, может быть выведена, например: если человек находится в помещении или на открытом воздухе, размер комнаты, в которой он говорит, материал окружающих стен, если есть окна, какое оборудование используется поблизости, и даже время суток на основе сигнатур, оставленных в записи колебаниями местной электрической сети.

Используя эти идеи, можно создать конструкцию лица или всего тела интересующего лица, обеспечив правоохранительным органам реалистичное и действенное представление. Эта технология позволяет получить прогноз будущих физических характеристик человека, скажем, через пять или десять лет, основываясь исключительно на голосовых записях.

Хотя это голосовое профилирование само по себе очень перспективно, оно ещё не было широко изучено правоохранительными органами, и только

предстоит пройти некоторый путь, прежде чем оно станет жизнеспособным в суде. Тем не менее, в 2014 году приложение для голосового профилирования, разработанное Университетом Карнеги-Меллона, сыграло важную роль в расследовании мистификационных сигналов бедствия береговой охране Соединённых Штатов, что привело к аресту[7]. Такие фальшивые сигналы бедствия являются федеральным преступлением в Соединённых Штатах и растрачивают государственные ресурсы и неоправданно подвергают риску жизнь береговой охраны.

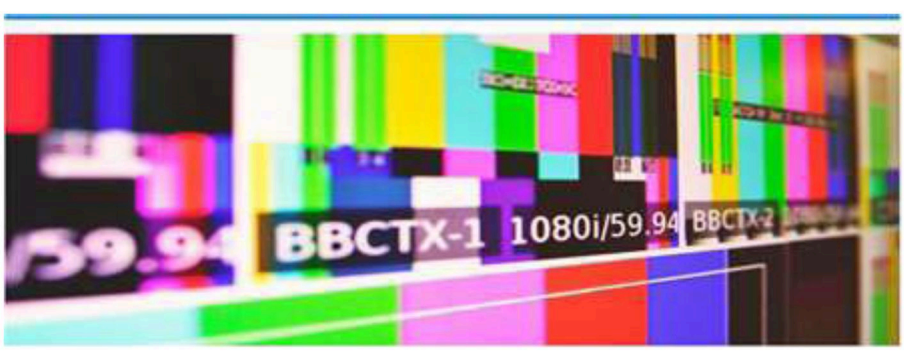
В этом случае, приложение голосового распознования использовалось для создания профиля вызывающего абонента, что помогало чиновникам устранить ложные наводки и, в конечном счёте, ускорить идентификацию субъекта и его местонахождение.

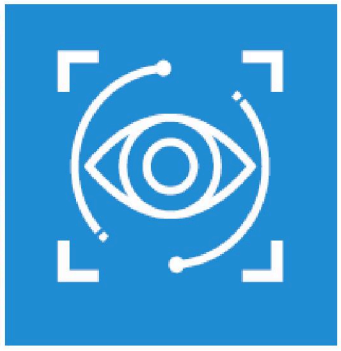
Однако для правоохранительных органов уместно отметить, что эта технология все ещё сталкивается с рядом практических проблем, включая:

- Ухудшение качества, возникающее при шумных условиях, неидеальных акустических средах и каналах;
- Перекрывающиеся человеческие голоса, такие как многократные одновременные разговоры, разговоры с нескольких динамиков и разговоры, происходящие в переполненных пространствах;
- С увлечением числа новых технологий, которые могут быть использованы для записи или передачи звука, каждая производит различные акустические сигнатуры;
- Манипуляция голосом или вокальный артистизм, который может замаскировать истинный голос говорящего;
- Появление голосовых приложений deepfake, которые могут генерировать поддельные голоса;
- Тенденция к снижению определённых диапазонов уникальных характеристик обусловлена такими факторами, как глобализация, новые технологии в средствах массовой информации и развлечений.

[7] Singh, R. (2019). Profiling Humans from their Voice. Carnegie Mellon University, Pittsburgh, Springer.

Визуальная обработка





В биологическом контексте визуальная обработка – это интерпретация и понимание визуальной информации, которая позволяет нам идентифицировать то, что мы видим, интерпретировать размер, форму, расстояние и т.д. С технической точки зрения, визуальная обработка, или компьютерное зрение, является имитацией зрительной системы человека машиной и касается извлечения, анализа и понимания информации из изображений.

Работа правоохранительных органов уже давно подкрепляется визуальной информацией – будь то фотографии или видеозаписи лиц, транспортных средств или мест, представляющих интерес. На самом деле правоохранительные органы очень сильно трансформировались с появлением технологий видеонаблюдения, в частности систем, которые стали широко доступны в 1960-е и 1970-е гг. Эта технология позволила правоохранительным органам быстро выявлять жертв, преступников или других лиц, представляющих интерес, и благодаря этому раскрывать преступления. Технологии наблюдения претерпели значительный прогресс за эти годы, включая появление персональных видеорегистраторов и патрульных беспилотников, но именно с ИИ, возможно, могут быть достигнуты самые впечатляющие результаты.

В последнее десятилетие, системы наблюдения, сопровождаемые крупными достижениями в области машинного обучения, создали системы, которые могут быть обучены более эффективно выполнять работу людей. Ранние системы машинного обучения для наблюдения были недостаточно развиты, поскольку они имели низкую производительность, требовали много времени и требовали высококвалифицированных инженеров для переобучения модели для каждого нового развёртывания. Однако с 2012 года глубокое обучение произвело революцию в области обработки изображений и распознавания объектов. Интеграция моделей глубокого обучения в системы наблюдения позволила добиться огромного прогресса в этой области, в частности за счёт улучшения обнаружения и анализа объектов, человеческих лиц и тел, что привело к существенному снижению частоты ошибок при

неправильной идентификации интересующих лиц. Эти продвинутые системы могут проводить распознавание и идентификацию лиц, а также определять мимику. Кроме того, они могут проводить обнаружение человеческого тела, идентификацию личности, распознавание атрибутов, распознавание поведения человека и распознавание движения тела (походки). Что касается объектов, то они могут осуществлять отслеживание объектов, идентификацию и повторную идентификацию транспортных средств, распознавание номерных знаков и классификацию места преступления. Системы визуальной обработки с поддержкой ИИ могут использоваться для выявления аномального поведения, а также для лиц, внесённых в чёрный или белый список, для облегчения или ограничения доступа в определённые здания или закрытые мероприятия, такие как концерты и фестивали. Это может существенно повысить готовность правоохранительных органов и сил безопасности, которым поручено охранять подобные мероприятия. В то же время эта область продолжает развиваться вместе с другими разработками, такими как системы поиска лиц на горизонте, которые могут использовать снимок человека для поиска через системы живых камер, чтобы найти их.

В последнее десятилетие системы наблюдения, сопровождаемые крупными достижениями в области приложений машинного обучения, создали системы, которые могут быть обучены выполнять работу людей более эффективно

Однако эти системы сталкиваются с рядом серьёзных практических проблем, включая нефронтальные предметы или закрытые предметы, а также использование аксессуаров для лица, таких как очки, ювелирные изделия и маски. Несмотря на это, эти системы будут только более продвинутыми с увеличением объёма данных и развитием методов распознавания, таких как метод идентификации лицевых точек, который позволит правоохранительным органам преодолеть эти проблемы при использовании технологий визуальной обработки.

Оптимизация ресурсов





Во времена, которые характерны всё более ограниченными ресурсами, всё более сложной оперативной средой и отсутствием существенного снижения уровня преступности в мире, правоохранительным органам всё чаще приходится делать больше работы с меньшими затратами. Исторически сложилось так, что правоохранительные органы использовали технологии для повышения эффективности полицейской деятельности, улучшения операций и материально-технического обеспечения в стремлении к созданию более эффективных систем реагирования, оптимизирующих необходимый объем ресурсов для конкретной ситуации. Оптимизация ресурсов – помощь правоохранительным органам делать больше с меньшими затратами – это ещё одна область, в которой ИИ может играть значительную роль.

Вместе с интеллектуальными датчиками, Интернетом вещей, телекоммуникационной сетью следующего поколения (5G, Wi-Fi 6) и дополненной реальностью, ИИ является ключом к реализации концепции «умной полиции», поддержке процессов стратегического планирования и принятия решений, повышению эффективности за счёт улучшения распределения сотрудников, транспортных средств и оборудования и сокращению времени реагирования на чрезвычайные ситуации. Технологические усовершенствования и усовершенствованные стратегии динамического согласования спроса и предложения ресурсов уже помогли сократить время реагирования на экстренные вызовы. Дальнейшее совершенствование этих динамических систем и процессов в идеале приведёт к повышению уровня безопасности. Хотя картирование преступности ведётся правоохранительными органами с 1990-х годов, данные и алгоритмы машинного обучения, необходимые для значительных прорывов, стали доступны только сейчас. Эти инструменты позволяют принимать хорошо обоснованные решения, чтобы значительно сократить время реагирования на чрезвычайные ситуации и укрепить связь между предупреждением, реагированием и реакцией.

В отношении использования ИИ для оптимизации ресурсов можно выделить пять основных областей:

- **Тепловая карта** – нанесение на карту горячих точек, сбор исторических данных о преступлениях от правоохранительных органов в сочетании с дополнительными наборами данных, включая прогнозы погоды, историю патрулирования полиции и учёт оперативной обстановки, для прогнозирования вероятных преступлений в той или иной части города.

- **Развёртывание ресурсов по требованию** – распределение полицейских ресурсов (то есть сотрудников, транспортных средств и оборудования) на основе фактической загруженности в местах, где прогнозируются преступления.

- **Планирование маршрутов патрулирования** – использование выявленных тепловой карты для оптимизации маршрутов и графиков патрулирования.

- **Формирование ресурсов** – отправка ближайших доступных сотрудников на вызовы службы, на основе их прогнозируемого времени отклика.

- **Построение маршрута** – определение оптимального маршрута, путём учёта расстояния и времени, а затем развёртывание ресурсов на основе доступности и оптимального времени отклика.

Технология оптимизации ресурсов в последние годы получила большое развитие и будет по-прежнему использоваться во многих операциях государственного управления, в том числе правоохранительными органами. Однако использование ИИ для оптимизации ресурсов требует, чтобы правоохранительные органы были готовы ответить на ряд существенных вопросов в процессе проектирования, которые будут определять эффективность этого инструмента.

В сущности, когда дело доходит до понимания и прогнозирования оптимальных решений, такая система должна знать, что такое «оптимальный способ» и как его вычислить. Кроме того, она должна знать, когда, где и как происходят инциденты; как могут быть развёрнуты ресурсы; насколько хорошо будут работать развёрнутые ресурсы; сколько времени займёт рассмотрение дел; как другие переменные, такие как трафик, время суток, время недели или погода, влияют на модели инцидентов. Надёжная оптимизация развёртывания также потребует планы, которые будут хорошо работать с несколькими сценариями инцидентов, и общая цель должна заключаться в минимизации неудачного реагирования на инциденты. Человеческими ресурсами необходимо

будет проводить постоянную оценку эффективности этих систем. Это можно сделать путём сравнения развёртываний, разработанных с использованием сгенерированных сценариев, проверенных на реальных данных.

В конечном счёте, оценки помогут улучшить системы, поскольку модель машинного обучения строится на прошлых успехах и неудачах.

Обработка человеческой речи



Распознавание человеческой речи (РЧР) – иначе называемое компьютерной лингвистикой – это область ИИ, которая, по сути, позволяет машинам читать, понимать и извлекать смысл из человеческих языков. Он оказался полезным при извлечении информации из больших наборов данных, особенно тех, которые содержат неструктурированные данные – данные, которые не содержатся или не могут содержаться в формате строки – столбца – как текст электронного письма. В свете этого РЧР нашло свое применение в повседневной жизни, например, во многих приложениях, которые обеспечивают прогностическую или суггестивную проверку текста и слов или грамматики.

В контексте правоприменения РЧР обладает значительным потенциалом, особенно в области анализа и классификации доказательств. Это может быть сделано путём извлечения информации и анализа из текстовых источников, таких как электронные письма, онлайн-чаты, письменные или печатные документы, или их изображения. Таким образом, правоохранительные органы могут сэкономить время и ресурсы на извлечении соответствующей информации из данных и преобразовании её в практическую информацию для цифровой криминалистики, чтобы помочь расследованиям.

Распознавание текста в речи может быть реализовано, что может быть одинаково выгодно для правоохранительных органов. Как только речь обнаружена в аудиодорожке, приложения НЛП могут быть использованы для выполнения звукового поиска или для создания автоматических расшифровок разговоров, которые могут быть полезны, например, для машин, принимающих заявления. После того, как аудио было расшифровано, текст может быть

обработан для извлечения информации, а именно путём классификации темы, настроения и намерения текста или путём кластеризации (т.е. – комплексы однородных и разнородных групп). Последние исследования все больше сосредотачиваются на неконтролируемом обучении, поскольку модели машинного обучения теперь способны понимать тему и контекст информации только с помощью текста, что открывает весь контент всемирной паутины для приложений РЧР. НЛП также имеет потенциал быть полезным в улучшении цифровой безопасности. Например, фильтры с поддержкой НЛП могут классифицировать и анализировать электронные письма, чтобы блокировать фишинговые атаки. В эпоху фальшивых новостей он также может помочь бороться с дезинформацией, определяя, является ли источник точным и заслуживающим доверия.

В контексте правоприменения РЧР обладает значительным потенциалом, особенно в области анализа и классификации доказательств

По этим причинам, некоторые правоохранительные органы приняли к сведению и начали работать с НЛП, чтобы обрабатывать и преобразовывать язык, а затем извлекать информацию для поиска в документах, обнаружения выраженных чувств, обобщения текстов и перевода между языками. РЧР, однако, является очень сложной задачей, и для разработки приложения РЧР требуется значительная работа.

К счастью, благодаря передаче знаний – совместному использованию частей кода скриптов, модельных модулей или библиотек для алгоритмов – эксперты могут помогать друг другу. Например, в Национальной полиции Нидерландов заметно активизировали проекты с открытым исходным кодом данных с целью повышения успешности и результатов НЛП, а также доступности использования этих технологий во благо. Благодаря передаче знаний эксперты смогут сотрудничать в целях укрепления практики и моделей, которые могут быть использованы правоохранительными органами.

3. Опыт исспользования правоохранительными органами

В ходе второго глобального совещания было признано, что со времени проведения совещания в 2018 году в области ИИ и правоприменения произошли значительные изменения, причём многие правоохранительные

органы существенно повысили свой интерес к ИИ. Этот рост отражается в числе случаев, когда государства приняли национальные стратегии, планы действий или соответствующие программные документы по ИИ[8]. Хотя не во всех этих стратегиях конкретно рассматриваются правоохранительные органы или предупреждение преступности в качестве компонента национального подхода к ИИ, в Германии[9], Италии[10], Литве[11], Нидерландах[12], Республике Корея[13] и Объединённых Арабских Эмиратах[14] это особенно заметно, хотя и очень кратко в большинстве случаев. Несмотря на краткость этих ссылок, такие признания начинают закладывать стратегическую основу для правоохранительных органов, изучающих развитие потенциала ИИ. Этот интерес к ИИ для правоохранительных органов проявился также в увеличении числа подразделений, центров и научно-исследовательских лабораторий, специализирующихся на ИИ, которые были недавно созданы правоохранительными органами. Например, группа больших данных в недавно созданном Центральном управлении информационных технологий в секторе безопасности Германии (ZITiS); лаборатория ИИ для обеспечения общественной безопасности (Ai-LECS), созданная Австралийской федеральной полицией в сотрудничестве с Университетом Монаша; а также команда машинного обучения и больших данных по планированию передовых технологий в японском Национальном полицейском агентстве (NPA). В соответствии с этим несколько правоохранительных органов приступили к изучению новых концепций и приложений в рамках пилотных проектов и повышению открытости к сотрудничеству и решению присущих этическим, правовым и социальным проблемам, связанных с использованием ИИ в правоохранительных органах.

---

[8] For a broad overview of State initiatives, refer to Campbell, T. (2019). Artificial Intelligence: An Overview Of State Initiatives. Retrieved from http://www.unicri.it/in_focus/files/Report_AI-An_Overview_of_State_Initiatives_FutureGrasp_7-23-19.pdf

[9] Federal Government of Germany (2018). Artificial Intelligence Strategy. Retrieved from https://www.bundesregierung.de/resource/blob/997532/1550276/3f7d 3c41c6e05695741273e78b8039f2/2018-11-15-ki-strategie-data.pdf?download=1 The Agency for Digital Italy (2018). Artificial Intelligence at the Service of Citizens. Retrieved from https://ia.italia.it/assets/whitepaper.pdf

[10] The Agency for Digital Italy (2018). Artificial Intelligence at the Service of Citizens. Retrieved from https://ia.italia.it/assets/whitepaper.pdf

[11] Ministry of Economy and Innovation of the Republic of Lithuania (2019). Lithuanian Artificial Intelligence Strategy: A Vision of the Future. Retrieved from http://kurklt.lt/wp-content/uploads/2018/09/StrategyIndesignpdf.pdf

[12] Ministry of Economic Affairs and Climate of the Netherlands (2019). Strategic Action Plan for Artificial Intelligence. Retrieved from https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/beleidsnotas/2019/10/08/strategisch-actieplan-voor-artificiele-intelligentie/Rapport+SAPAI.pdf

[13] Government of the Republic of Korea (2017). Mid- to Long-Term Master Plan in Preparation forthe Intelligent Information Society. Retrieved from https://k-erc.eu/wp-content/uploads/2017/12/Master-Plan-for-the-intelligent-information-society.pdf

[14] Government of the United Arab Emirates (2017). UAE Strategy for Artificial Intelligence. Retrieved from https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/uae-strategy-for-artificial-intelligence

В ходе второго глобального совещания для правоохранительных органов были определены конкретные обновлённые данные по случаям использования ИИ и изучаемым НИОКР.

Неинтрузивные сиситемы видеонаблюдения

Норвегия

Видеозаписи и изображения, собираемые правоохранительными органами с помощью систем видеонаблюдения, таких как замкнутое телевидение (CCTV) и камеры кузова или автомобиля, часто необходимы правоохранительным органам для предотвращения и расследования преступлений, а также обеспечения судебного преследования правонарушителей в рамках судебной системы. Однако в то же время изображения, видео и звуки содержат информацию, которая может раскрыть личность отдельных лиц, обработка и использование которой может вызвать вопросы в отношении конфиденциальности. Хотя ненавязчивая слежка открывает перед правоохранительными органами и обществом возможности для переосмысления наблюдения, она, тем не менее, по-прежнему требует тщательного рассмотрения вопросов конфиденциальности, защиты данных, деанонимизации и практических аспектов использования анонимизированных данных правоохранительными органами.

Изображения, видео и звуки содержат информацию, которая может раскрыть личность отдельных лиц, обработка и использование которой может вызвать озабоченность в отношении конфиденциальности

Стремясь к прозрачности, норвежский полицейский округ Осло работает с партнёрами как внутри полиции, так и за её пределами с промышленностью и академическими кругами, изучая применение ИИ для создания сильно чувствительных к пользователю неинтрузивных систем наблюдения, которые могут быть использованы в умных городах.

В основе этого лежит анонимизация видео и изображений, собранных с помощью ИИ. Более конкретно, изображения людей, снятые на видеокадрах наблюдения, автоматически анонимизируются системой ИИ, покрывая их лицо мультяшным персонажем или эмодзи. Это позволяет анонимным наборам данных обрабатываться и совместно использоваться полицией и её партнёрами для использования в ненавязчивой манере, например, анонимизированные данные могут использоваться для анализа уличных драк или движений, указывающих на опьянение. Проект знаменует собой одно из первых

испытаний правоохранительных органов, в котором распознавание образов сочетается со средствами автоматической анонимизации. Этот пилотный проект также примечателен тем, что он может даже представить частичное решение проблемы соблюдения общего регламента защиты данных Европейского союза (ЕС), в соответствии с которым правоохранительные органы должны иметь возможность осуществлять ненавязчивый мониторинг и анализ доказательств в отношении конфиденциальности «случайных прохожих» или лиц, не представляющих интереса (non-POI)[15].

Пока ненавязчивое наблюдение предоставляет провоохранительным органам и обществу возможности для переосмысления наблюдения, оно, тем не менее, по-прежнему требует тщательного рассмотрения вопросов конфиденциальности, защиты данных, деанонимизации и практических аспектов исользования анонимизированных данных правоохранительными органами.

Данные AIRLOCK и распознавание нежелательных материалов

Австралия

В Австралии Австралийская федеральная полиция (AFP) изучает несколько возможностей использования ИИ и машинного обучения для автоматизации или оказания помощи в решении таких задач, как маркировка и организация данных. Это включает в себя создание поисковой системы, подобной Google, для поиска данных, которые будут поддерживать AFP в том, чтобы иметь смысл и использовать большие объёмы структурированных и неструктурированных данных в своих базах данных. В противном случае без поддержки таких инструментов он может столкнуться с трудностями в поиске точек данных и создании критических соединений. Ещё одна тема, над которой работает AFP, – это создание системы «шлюза данных», что позволяет исследователям разрабатывать новые алгоритмы, не имея доступа к данным. Шлюз данных оснащён криптографией, чтобы обеспечить изолированную и безопасную среду, в которой исследователи могут поместить свои алгоритмы и модели, выполнить их против данных и извлечь результаты исследований и анализа. Соответственно, данные никогда не покидают среду владельца данных, что особенно актуально для организаций, имеющих дело с конфиденциальными данными. Ожидается, что система шлюзования данных позволит третьим сторонам обучать, проверять и тестировать средства

[15] See GDPR, inter alia, Article 5(1)(c), which sets the 'data minimisation' principle. The full text of the GDPR is available at https://gdpr-info.eu

машинного обучения на основе реальных захваченных данных, не требуя прямого доступа к этим материалам. Это могло бы, например, помочь исследователям лучше понять и контролировать «даркнет». Заметное применение этой системы, которое изучается AFP фокусируется на использовании моделей глубокого обучения для распознавания, маркировки и кластеризации изображений и видео, содержащих вредоносные материалы, такие как сексуальное насилие над детьми. Автоматизированное распознавание вредных материалов в сочетании с данными воздушного шлюза, эффективно защитит сотрудников правоохранительных органов, следователей и исследователи от воздействия этих материалов.

Шлюз данных оснащён криптографией, чтобы обеспечить изолированную и безопасную среду, в которую исследовател и могут поместить свои алгоритмы и модели, выполнить их против данных и извлечь результаты исследований и анализа.

Система рекомендаций

Германия

Центральное управление информационных технологий в секторе безопасности (ZITiS) при Федеральном министерстве внутренних дел Германии работает над системой рекомендаций, аналогичной тем, которые используются такими платформами, как Amazon, Netflix и Spotify. Рекомендательные системы работают на предположении, что в больших, разнообразных наборах данных похожие пользователи выбирают похожие элементы. На основе этих знаний, а также после начального периода обучения, элементы, представляющие потенциальный интерес, автоматически рекомендуются пользователю.

Для больших баз данных правоохранительных органов, содержащих огромное количество данных уголовных расследований, поиск соответствующей информации часто подобен поиску пресловутой «иголки в стоге сена». ZITiS был специально мотивирован к разработке рекомендательной системы для удовлетворения потребностей современных расследований финансовых преступлений, которые обычно требуют тщательного изучения огромного количества финансовых данных. Крупные дела такого рода могут занять годы работы по поиску и перекрёстной проверке соответствующей информации для случая. С увеличением объёма данных и постоянно расширяющихся баз данных частота возникновения таких крупных случаев, вероятно, возрастёт. Сама система является активным обучающим

инструментом на основе контента, что означает, что алгоритм пытается интерактивно запрашивать ценную информацию для офицеров на основе предыдущих поисков или аналогичных предпочтений пользователей.

Поиск нужной информации в больших базах данных правоохранительных органов часто напоминает поиск пресловутой «иголки в стоге сена».

Существуют некоторые проблемы, связанные с созданием эффективных систем рекомендаций, необходимо, чтобы рекомендательная система с возможностями принятия решений не была предвзятой. Предвзятость повлияет на точность и правдивость информации и может поставить под угрозу расследование. Это будет серьёзной проблемой для правоохранительных органов, чтобы тщательно ориентироваться, поскольку рекомендательные системы на самом деле предназначены для поощрения пользователей в определённом направлении, чтобы избежать поиска в нескольких направлениях.

Например, рекомендательные системы в частном секторе, такие как Amazon, Netflix и Spotify, призваны стимулировать пользователей «покупать больше продуктов», «смотреть больше фильмов» или «слушать больше музыки».

Правоохранительным органам необходимо будет обеспечить, чтобы их рекомендательные системы действительно были ориентированы на предоставление ценной информации, а не просто поощрялись «новые аресты». Другая проблема заключается в том, что обычные рекомендательные системы используют ограниченные типы данных, такие, как аудио или видео исключительно в то время, как с правоохранительными органами эти системы должны были бы работать с очень широким диапазоном типов данных, таких как электронные письма, изображения, аудио, видео.

Другие потенциальные проблемы включают в себя обеспечение создания точных метаданных, разнообразие контента, добавление и контекстуализацию нового контента, объяснение рекомендаций и «холодный старт» – связывая случаи, отдельных лиц и доказательства, которые могут быть актуальными.

Скрининг крупных событий, наблюдение и многое другое

Япония

Правительство Японии начало сотрудничество с несколькими технологическими компаниями в рамках политики развития ИИ, направленной на обеспечение максимальной безопасности и предотвращение преступности и терроризма, ставящих под угрозу проведение массовых мероприятий.

Например, в качестве следующей принимающей страны Олимпийских игр – мероприятия, которое, как ожидается, соберёт около 600000 иностранных гостей, – укрепление безопасности является главным приоритетом для национальных властей Японии, включая Национальное полицейское агентство (НПА). В апреле 2019 года НПА учредила новый офис «планирования передовых технологий», которыйстремится использовать выгодное использование передовых технологий, таких как ИИ.

Используя методы глубокого обучения, полиция префектуры разрабатывает инструмент для обнаружения, анализа и прогнозирования места и времени вероятных преступлений, и несчастных случаев на основе статистических данных и соответствующих каналов данных

Исследовательский центр полицейской информации и коммуникаций Национальной полицейской академии дополнительно изучает три пилотных приложения, которые могли бы укрепить безопасность массовых мероприятий. Они включают в себя использование ИИ для идентификации моделей автомобилей на кадрах видеонаблюдения, анализа подозрительных финансовых операций, которые могут указывать на отмывание денег и оказания помощи в выявлении движений или действий, которые могут считаться подозрительными. Полиция префектуры Токио аналогичным образом разрабатывает в экспериментальной форме инструменты с поддержкой ИИ, ориентированные на выявление районов с высоким уровнем риска преступности, которые могут помочь в определении оптимальных маршрутов патрулирования или методов предупреждения преступности.

Правоохранительные органы в других префектурах Японии, таких как Канагава, также работают над статистикой горячих точек, чтобы информировать полицию. Используя методы глубокого обучения, полиция префектуры разрабатывает инструмент для обнаружения, анализа и прогнозирования места и времени вероятных преступлений и несчастных случаев на основе статистических данных и соответствующих каналов данных.

Чтобы сделать эти прогнозы, инструмент учитывает такие факторы, как время суток, место, погода, географическое состояние, городская мобильность и различные каналы данных о прошлых преступлениях и несчастных случаях в этом районе, а также знания оперативной обстановки. Подобная деятельность помогает сотрудникам полиции выявлять закономерности преступлений и несчастных случаев; обеспечивает целостный обзор при активном расследовании преступлений; и, наконец, снижает вероятность совершения преступлений путём внедрения усовершенствованного маршрута патрулирования.

4. Ответственность при исспользовании ии

В первом докладе Интерпола – ЮНИКРИ об ИИ для правоохранительных органов были широко представлены правовые и этические перспективы использования ИИ правоохранительными органами, а также сделано предостережение о том, что правоохранительные органы должны обеспечивать ответственное использование данного иструмента. Хотя настоящий доклад призван носить практический и оперативный характер, полезно с самого начала уточнить термин «ответственный», чтобы избежать двусмысленных толкований. Основополагающая Белая книга 2019 года AI and Ethics at the Police Лейденского университета и TU Delft[16] предполагает, что с юридической точки зрения действовать ответственно означает «принимать моральную целостность и подлинность в качестве идеалов и приложить разумные усилия для их достижения[17]«. Стремление к нравственной целостности, в свою очередь, подразумевает «приверженность ценностям свободы, равенства и солидарности[18]. Однако для целей настоящего доклада будет принято более чёткое понимание, и термин «ответственный» будет сформулирован в соответствии с Оксфордским словарём, который определяет «ответственный» как действующий «разумным или заслуживающим доверия образом[19]«. В этом контексте ответственное использование правоохранительными органами следует понимать, как использование, закрепляющее общие принципы уважения прав и свобод человека, демократии, справедливость и верховенство закона. Для достижения этих принципов правоохранительные органы должны

---

[16] Zardiashvili, L., Bieger, J., Dechesne F. and Dignum, V. (2019). AI Ethics for Law Enforcement: A Study into Requirements for Responsible Use of AI at the Dutch Police. Delphi.

[17] Dworkin, R. (2011). Justice for Hedgehogs. The Belknap Press, 111.
Ministry of Social Affairs and Employment. (2014). Core Values of Dutch Society. Pro Demos, House of Democracy and Constitution.

[18] Retrieved from https://www.prodemos.nl/wp-content/uploads/2016/04/ KERNWAARDEN-ENGELS-S73-623800.pdf

[19] Responsibly. (2019). In Oxford Online Dictionary. Retrieved from https://www.lexico.com/en/definition/responsibly

работать над тем, чтобы гарантировать, что разработка и использование ИИ соответствует требованиям справедливости, подотчётности, прозрачности и лёгкость восприятия (FATE). Эти требования возникли в последние годы в результате консенсуса в сообществе ИИ относительно того, что требуется алгоритмам, чтобы оправдать доверие к ним и гарантировать надлежащий уровень безопасности. Ниже приводится краткое объяснение каждого требования.

Справедливость подразумевает, что алгоритмические решения не оказывают дискриминационного или несправедливого воздействия на конечных пользователей. Автоматизированное решение не должно приниматься на основе таких признаков, как этническая принадлежность, пол, сексуальная ориентация, поскольку они могут привести к дискриминации.

В то же время простое уклонение от этих признаков не является решением, поскольку они, тем не менее, могут быть косвенно выведены из других критериев. Например, даже если этническая принадлежность не является критерием, если люди определённой этнической принадлежности живут в определённом районе и «адрес» является критерием, модель все равно может дать несправедливое определение. Справедливость требует, чтобы все системы ИИ подвергались строгому аудиту на предмет соблюдения права на недискриминацию, и в случае возникновения дискриминации должны быть приняты меры по обеспечению права на эффективное средство правовой защиты.





Подотчётность можно понимать, как ответственность за принятое действие и способность предоставить удовлетворительное обоснование для

этого. Правовая система построена на фундаментальном предположении о человеческих действиях, и поэтому замена их автономными, такими как ИИ. Учитывая сложность привлечения автономной системы, необходимо задать вопрос о том, кто несёт ответственность за действия, принятые системой ИИ? Это разработчик, производитель или конечный пользователь? Подотчётность требует разработки чётких правил ответственности и правовых инструментов для рассмотрения дел с автономными агентами.



Прозрачность включает в себя предоставление чёткой информации о принятых человеческих решениях.

Это включает в себя такие вопросы, как:

- Какова цель использования ИИ в конкретном контексте?
- Какие решения полностью автоматизированы?
- Какая модель машинного обучения используется?
- Какие данные используются?
- Какие объекты в наборе данных рассматриваются?
- Рассматриваются ли какие-либо из чувствительных индивидуальных атрибутов?
- Как соблюдается конфиденциальность данных?
- Прозрачность требует, чтобы такие вопросы, как конфиденциальность этих данных, соблюдались. Прозрачность требует, чтобы вопросы, подобные этим, были чётко проработаны, и чтобы те, кто внедряет систему ИИ, могли на них ответить.



Лёгкость восприятия тесно связана с требованием «прозрачности». Суть в том, чтобы алгоритмические решения могли восприниматься конечными пользователями в нетехнических терминах. Это касается так называемой «проблемы чёрных ящиков».

Системы глубокого обучения – это буквально чёрные ящики, которые объединяют и рекомбинируют атрибуты многими произвольными способами. Восприятие требует, чтобы пользователи могли интерпретировать информацию, извлечённую из чёрного ящика, и понимали, какие элементы, используются в модели машинного обучения.

В отличие от других требований справедливости, подотчётности, прозрачности, «лёгкость восприятия» - это очень большая техническая проблема для разработчиков и производителей. Однако несколько групп работают над разработкой инструментов, которые могут ясно и наглядно объяснить какие признаки в данных были наиболее важны для модели, а также влияние каждого фактора на конкретный результат[20].

Помимо этих четырёх требований, концепции безопасности и надёжности также часто поднимаются с точки зрения общей надёжности систем ИИ и их устойчивости к атакам, а также с точки зрения безопасности. Эти дополнительные требования также должны быть тщательно учтены правоохранительными органами в отношении собственного ИИ. Для

[20] Kaur, H., Nori, H., Jenkins, S., Caruana, R., Wallach, H. and Wortman Vaughan J. (2020). Interpreting interpretability: Understanding data scientists' use of interpretability tools for machine learning. University of Michigan, Microsoft Research.

обеспечения того, чтобы системы ИИ были одновременно безопасными и надёжными, при разработке и развёртывании систем ИИ необходимо институционализировать две основные практики: во-первых, периодическую целостность системы и обновление её как внутренними инженерами, так и сотрудниками полиции (являющимися пользователями) и, при необходимости, надёжным внешним партнёром; во-вторых, возможность интероперабельности, которая может быть понята как обеспечение того, чтобы система была «проста в эксплуатации» офицерами и «осуществима для использования с другими будущими системами».

Если при использовании ИИ правоохранительными органами граждане почувствуют угрозу, обнаружат методы работы, противоречащие принципам и требованиям этики и даже законности, вероятно, проявится неблагоприятная реакция. Это может вызвать сопротивление и громкую критику использования приложений ИИ и других передовых технологий правоохранительными органами. Для предотвращения этого и обеспечения того, чтобы правоохранительные органы могли продолжать использовать позитивный потенциал ИИ, необходимо сохранять общественное доверие.

Учитывая важность этого вопроса, в ходе второго глобального совещания была организована серия панельных презентаций для более глубокого изучения некоторых правовых и социальных аспектов использования ИИ правоохранительными органами, а также некоторых изменений в ведущемся этическом дискурсе. Следующие разделы были основаны на данных презентациях.

3.1 Законность

Существуют значительные правовые проблемы для правоохранительных органов в области ИИ. Если не получится это преодолеть, использование ИИ может нарушить основные права человека, такие как право на неприкосновенность частной жизни, равенство и недискриминацию, а также подорвать принципы права, такие как презумпция невиновности, защита от самообвинения. Прежде всего, эти проблемы требуют, чтобы правоохранительные органы следили за тем, чтобы использование ИИ соответствовало закону. Учитывая, что ИИ подпитывается данными, это касается, в частности, законов, касающихся конфиденциальности данных, которые включают в себя правила сбора, защиты и обработки данных. Кроме того, правоохранительные органы должны не только обеспечивать соблюдение закона во время использования любых систем ИИ, но и обеспечивать, чтобы это имело место в контексте их развития. Существует два всеобъемлющих

правовых документа, которые регулярно возникают в ходе дискуссий об использовании ИИ не только правоохранительными органами, но и другими сообществами конечных пользователей, а именно: Общий регламент ЕС по защите данных (GDPR) и Директива ЕС по правоохранительным органам 2016/680 (LED)[21]. Хотя ни один из этих инструментов не был разработан специально для ИИ, но поскольку они касаются данных, они в конечном итоге имеют непосредственное отношение к разработке и внедрению ИИ. Кроме того, учитывая, что GDPR касается личной информации граждан ЕС и в этом отношении применима к организациям, действующим как внутри ЕС, так и за его пределами, GDPR, в частности, является инструментом глобального значения и заслуживает пристального внимания.

Принятый Европейским парламентом и Европейским советом в апреле 2016 года и впоследствии вступивший в силу в мае 2018 года, GDPR является результатом более чем четырёхлетнего обсуждения и переговоров, и был разработан для модернизации законов, защищающих личную информацию физических лиц.

Он содержит шесть основных принципов сбора и обработки персональных данных:

- законность, справедливость и прозрачность;
- ограничение целей;
- минимизация данных;
- точность;
- ограничение хранения;
- целостность и конфиденциальность (безопасность)[22].

Директива LED, также известная как директива полиции, вступила в силу в мае 2016 года и направлена на применение правил, регулирующих персональные данные в GDPR, к деятельности правоохранительных органов. Она была высоко оценена за её роль в создании «зоны свободы, безопасности и справедливости с высоким уровнем защиты данных в соответствии с Хартией основных прав ЕС».»Направленный на защиту персональных данных физических лиц и гарантирующий высокий уровень общественной безопасности, закон предусматривает права субъектов персональных данных, а также обязанности «компетентных органов» при обработке данных в «правоприменительных целях», то есть предупреждении, расследовании,

---

[21] See EU Law Enforcement Directive 2016/680 available at 21 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680

[22] See GDPR Article 5(1), which sets out the six principles.

раскрытии, преследовании уголовных преступлений или исполнении головных наказаний, это включает в себя защиту от угроз общественной безопасности и их предотвращение.

Как уже отмечалось, ни GDPR, ни LED не были приняты в отношении ИИ, и, следовательно, некоторые важные положения ещё предстоит проверить в контексте ИИ в полицейской деятельности. В этой связи возник ряд возможных ситуаций, связанных с требованиями GDPR и LED, которые вызвали значительные дебаты[23].

Сфера применения ограничений на автоматизированную обработку данных в соответствии с GDPR и LED является одной из тем для обсуждения. Решения, основанные исключительно на автоматизированной обработке, так называемые автоматизированные системы принятия решений (АДМ), которые всё чаще используются в прогнозной полиции для анализа данных, чтобы помочь предсказать, где будут совершаться преступления или кто будет вовлечён в преступление, вызывают практические проблемы с точки зрения ответственности и подотчётности. Приемлемость АДМ в суде также является спорной.

Хотя в GDPR прямо не упоминается ИИ, в нём содержится Положение о роли автономного принятия решений и, согласно статье 22, подразумевается право на объяснение автоматизированного принятия решений, включая профилирование, что означает, что «контроллеры должны будут проектировать, разрабатывать и применять свои алгоритмы прозрачным, предсказуемым и поддающимся проверке образом». Интересно, что в GDPR говорится, что субъект данных имеет право не подчиняться решению, основанному исключительно на автоматизированной обработке, за исключением случаев, когда оно основано на явном согласии субъекта данных. В этом контексте участникам должна предоставляться адекватная информация и/или там, где это возможно, должны использоваться общие или синтетические данные.

LED также конкретно охватывает системы АДМ в соответствии со статьёй 11, которая предусматривает, что системы АДМ, которые оказывают неблагоприятное правовое воздействие на субъекты данных или существенно влияют на него, должны быть запрещены, если только это не разрешено законодательством ЕС или государства – члена, в соответствии с которым контролёр является субъектом и которое обеспечивает соответствующие гарантии прав и свобод субъекта данных – по крайней мере право на получение человеческого вмешательства со стороны контролёра для выражения своей

[23] Hidvegi, F. Masse, E. (2018, Nov 1). Mapping regulatory proposals for artificial Intelligence in Europe. Retrieved from https://www.accessnow.org/cms/assets/uploads/2018/11/mapping_regulatory_proposals_for_AI_in_EU.pdf

точки зрения и оспаривания решения. Однако в соответствии с LED профилирование, приводящее к дискриминации физических лиц на основе обработки конфиденциальных данных, ни при каких обстоятельствах не может быть санкционировано.

Таким образом, для того, чтобы обеспечить эффективную правовую защиту, правоохранительные органы должны быть в состоянии предоставить объяснение индивидуального решения, а не только логику, лежащую в его основе, что может оказаться трудным в случае систем АДМ.

В свете трудностей, с которыми могут столкнуться правоохранительные органы при попытках ориентироваться в этих правовых аспектах, юристы должны быть вовлечены в процессы разработки и использования ИИ. Особенно это относится к тем случаям, когда системы АДМ рассматриваются для использования в процессе принятия решений с целью обеспечения того, чтобы не возникало никаких неблагоприятных последствий в отношении субъекта данных или любых других лиц. Кроме того, в свете некоторых правовых пробелов правоохранительные органы и другие соответствующие национальные органы, возможно, пожелают рассмотреть вопрос о разработке конкретных и/или корректировке существующих нормативных актов правоохранительных органов по использованию ИИ для определения и руководства тем, как он должен законно действовать, с учётом существующих инструментов глобального интереса, таких как GDPR и LED.

3.2 Общественное восприятие



Будучи относительно новой технологией, люди часто не до конца осознают, как на самом деле работает ИИ и плохо понимают его возможности. Это провоцирует беспокойство, страх и недоверие. При определённых обстоятельствах это чувство может препятствовать интеграции и применению технологии. Пожалуй, нигде это не является более критичным, чем, когда речь заходит об использовании ИИ в государственном секторе и, в частности, в правоохранительных органах. Эффективность правоохранительной системы зависит от доверия общества. Общественная безопасность может быть

поставлена под угрозу, когда общество теряет доверие к правоохранительным органам. В связи с этим общественное признание использования ИИ имеет первостепенное значение, поскольку правоохранительные органы всё больше интегрируют ИИ. Крайне важно, чтобы правоохранительные органы попрежнему осознавали необходимость этого, а также важность коммуникации и обмена информацией с ключевыми заинтересованными сторонами и широкой общественностью. Опрос, проведённый в 2018 году Центром высших исследований Министерства внутренних дел Франции, университетом Жан-Мулен Лион 3, французским Национальным полицейским колледжем и французским Национальным жандармским колледжем, изучал общественное мнение путём оценки доверия к построению анализов полицейской деятельности субъектами национальной безопасности[24]. Из всех приложений ИИ, изучаемых правоохранительными органами, полицейское прогнозирование регулярно является источником наибольшей озабоченности. Проект включал в себя публичный опрос более 2000 человек об общественных знаниях и мнениях о прогнозируемом полицейском управлении – как до, так и после него.

Результаты показали, что после объяснения объёмом в 150 слов граждане стали на 28% увереннее относиться к правоохранительным органам, использующим прогностическое полицейское управление, – рост с 59% до 87%. Более конкретно, это включало увеличение числа респондентов, согласившихся с тем, что прогнозирующая полицейская деятельность может быть полезна для предотвращения преступлений. После получения объяснений, также наблюдалось увеличение числа респондентов, согласных с тем, что прогнозирующая полицейская деятельность не представляет угрозу гражданским свободам. Кроме того, 59% респондентов указали, что они даже согласились бы на проверку личности исключительно на основании прогностического программного обеспечения правоохранительной деятельности. Эти результаты свидетельствуют о важности работы с населением. Общественное признание прогностической полицейской деятельности в этом случае не обязательно должно быть полностью мотивировано вновь приобретённым, рациональным и объективным пониманием или оценкой нюансов технологии. Вместо этого он может быть мотивирован исключительными обстоятельствами, такими как череда террористических инцидентов во Франции в период с 2015 по 2018 год, которые предшествовали опросу, или дезинформацией относительно технологии. Что касается дезинформации, то следует отметить исследование, которое показало, то что 44% респондентов оправдали использование прогностической полицейской деятельности для борьбы с терроризмом, хотя само по себе это не является первостепенной целью технологии.

---

[24]Piotrowicz, C. (2018). Predictive Policing: European Law Enforcement Research Bulletin, (4 SCE), 107-111. Retrieved from https://t cepol.europa.eu/index.php/bulletin/article/view/374

Коммуникация и обмен информацией, очевидно, являются важнейшими способами повышения общественного признания использования ИИ правоохранительными органами, но есть и несколько других способов. К ним относятся: разработка законодательства или реализация существующего; установление баланса между тем, какой объём данных необходим и достаточен для получения полезного результата, и тем, какой объём деталей является чрезмерным по отношению к целям процессов – так называемый принцип минимизации данных; анонимизация данных или использование фиктивных или общих данных везде, где это возможно; поиск и получение явного согласия участников или субъектов данных; а также вовлечение общественности – особенно уязвимых групп – в разработку и использование систем ИИ.

Наконец, важно, чтобы системы ИИ, построенные для правоохранительных органов, разрабатывались и развёртывались с учётом того, что ошибки нельзя полностью предотвратить и что ошибки могут неизбежно возникнуть. Соответственно, с самого начала следует разработать и обсудить с общественностью сценарий оценки рисков и смягчения их последствий.

3.3 Этика ИИ в ЕС

В последнее время на территории ЕС произошло несколько примечательных событий, благодаря которым Европейская комиссия стремилась решить эти этические, правовые и социальные проблемы, а также обеспечить, чтобы системы ИИ оставались ориентированными на человека и всегда были направлены на максимизацию преимуществ этой технологии при одновременном предотвращении или минимизации её рисков. В апреле 2018 года 24 государства – члена ЕС подписали декларацию о сотрудничестве в области ИИ, в рамках которой была выявлена необходимость разработки адекватной правовой и этической базы и сотрудничества с этой целью[25]. После этого в июне 2018 года Европейская комиссия учредила экспертную группу высокого уровня по ИИ (AI-HLEG) – независимую группу, состоящую из 52 видных представителей академических кругов, промышленности и гражданского общества. Перед группой была поставлена задача разработать рекомендации по разработке будущей политики, а также по этическим, правовым и социальным вопросам, связанным с ИИ, включая социально-экономические проблемы. С этой целью AI-HLEG опубликовала свои этические рекомендации для заслуживающих доверия ИИ в апреле 2019 года[26]

[25] European Union (2018). Declaration on Cooperation on Artificial Intelligence. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50951

[26] High-Level Expert Group on AI (2019). Ethics Guidelines for Trustworthy AI. Retrieved from https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

Европейская комиссия не является первым игроком, выпустившим такие руководящие принципы, этические руководящие принципы знаменуют собой первую правительственную инициативу в этой области и являются важным шагом на пути к тому, чтобы вывести на глобальный уровень не только антропоцентрический подход к ИИ, но и сформировать международный консенсус вокруг понятия этики ИИ.

Согласно руководящим принципам этики, для того чтобы ИИ считался заслуживающим доверия, он должен на протяжении всего своего жизненного цикла быть:

- законным, что влечёт за собой соблюдение всех применимых законов и правил;
- этичным, что направлено на обеспечение соответствия этическим нормам;
- надёжным, как с технической, так и с социальной точки зрения.

Развитие надёжных систем ИИ должно основываться на установленных фундаментальных ценностях, таких как уважение человеческого достоинства, демократия, справедливость и верховенство закона, и в то же время гарантировать свободу личности и права граждан в целях обеспечения равенства и недискриминации. Исходя из этого, этические руководящие принципы представляют собой четыре всеобъемлющих этических принципа, лежащих в основе разработки, развёртывания и использования систем ИИ: уважение человеческой автономии; предотвращение вреда; справедливость и лёгкость восприятия.



Естественно, что при попытке применить эти принципы на практике, между ними может возникнуть определённое напряжение. Рассмотрим, как отмечено в руководстве по этике, использование ИИ для прогнозирования полицейской деятельности. Хотя это может способствовать сокращению преступности, оно может также повлечь за собой наблюдение, которое посягает на личную свободу и неприкосновенность частной жизни, тем самым создавая конфликт и нарушая принцип предотвращения вреда. Этот вопрос требует обсуждения для поиска наиболее подходящего компромисса. Необходимо позаботиться о том, чтобы надлежащим образом выявлять, оценивать, документировать и сообщать об этих компромиссах и их решениях методическим образом.

Далее определяется ряд из требований к разработке, развёртыванию и использованию систем ИИ, а именно: кадровое обеспечение и надзор; техническая надёжность и безопасность; конфиденциальность и управление данными; прозрачность; разнообразие; недискриминация и справедливость; социальное и экологическое благополучие; подотчётность. Для выполнения этих требований этические руководящие принципы содержат как технические, так и нетехнические методы. Что касается первого, то заслуживающие доверия архитектуры ИИ должны реализовывать этику и верховенство закона по дизайну и конфиденциальность по дизайну, а также тесты для проверки системы и показателей качества обслуживания. К нетехническим методам реализации требований относятся: регламентация; кодексы поведения; стандартизация; сертификация; а также участие и усилия с точки зрения подотчётности, например, через рамки управления, просвещения и повышения осведомлённости в целях содействия этическому мышлению, участие заинтересованных сторон, социальный диалог и создание разнообразных и инклюзивных проектных групп. В дополнение к этим требованиям руководство по этике также содержит оценочный список или ряд неисчерпывающих вопросов, предназначенных для практической реализации ключевых требований и определения того, может ли ИИ в любом конкретном случае использования считаться заслуживающим доверия в соответствии с руководящими принципами по этике.

В июне 2019 года Европейская комиссия опробовала оценочный список, предложив заинтересованным сторонам протестировать его и предоставить обратную связь для включения в пересмотр оценочного списка. Примечательно, что с точки зрения правоохранительных органов, Национальная полиция Нидерландов участвовала в экспериментальном этапе.

В феврале 2020 года Европейская комиссия выпустила Белую книгу по ИИ –европейскому подходу к совершенству и доверию, которая сигнализирует о начале процесса разработки возможного законодательства об ИИ в ЕС.

Примечательно, что Белая книга опирается на основную работу, проделанную AI-CHALLENGE в области развития уважения основных прав и ценностей. Он также предлагает конкретные правовые требования, такие как обучение ИИ репрезентативным данным, ведение компаниями подробной документации о том, как был разработан ИИ, и информирование граждан о том, когда они взаимодействуют с системой ИИ.

Очевидно: что Европейская инициатива, руководящие принципы и любые последующие усилия по их дальнейшей практической реализации в форме законодательства ЕС, скорее всего, выйдут за пределы Европы. Как отмечают сами руководители, их цель состоит в том, чтобы способствовать размышлению и обсуждению этических рамок для ИИ на глобальном уровне. В этой связи следует особо отметить актуальность данного европейского подхода к созданию надёжных систем ИИ на службе человечества.

Другие инициативы в области этики ии

Дискуссии об этике ИИ и развитии ответственного ИИ в соответствии с основными правами не ограничиваются Европой[27]. Несколько организаций государственного сектора, научно-исследовательских институтов и частных компаний выпустили заявления о принципах или создали экспертные комитеты по ИИ для подготовки проектов программных документов о том, как подходить к ИИ. Недавнее исследование Nature выявило 84 документа, содержащих этические принципы или руководящие принципы для ИИ[28]. Несмотря на возможность дублирования, каждый из этих документов сам по себе является ценным инструментом и представляет собой точку отсчёта для правоохранительных органов, продвигающихся вперёд в ответственном развитии и применении ИИ.

Наиболее примечательно, что Организация экономического сотрудничества и развития (ОЭСР) учредила в мае 2018 года экспертную группу для разработки принципов ИИ в обществе и впоследствии приняла свои акты по ИИ в мае 2019 года – «Первый свод межправительственных руководящих принципов политики в области ИИ»[29]. Договорённости, которые были приняты 42 государствами, основаны на намерении продвижения ИИ. ИИ представляется инновационным и заслуживающим доверия, который уважает

---

[27] European Commission (2020). White Paper: On Artificial Intelligence - A European Approach to Excellence and Trust. Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[28] Jobin, A., lenca, M. & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence 1,389-399.

[29] OECD. (2019). Principles on Artificial Intelligence. Retrieved from https://www.oecd.org/going-digital/ai/principles/

права человека и демократические ценности. На национальном уровне было также создано несколько комитетов и групп экспертов для изучения этических аспектов ИИ, таких как консультативный совет по этическому использованию ИИ и данных в Сингапуре и специальный комитет по ИИ Палаты лордов Соединённого Королевства.

Аналогичные усилия предпринимаются и в частном секторе, особенно среди корпораций, которые полагаются в своей деятельности на ИИ.

В частности, крупные отраслевые компании, такие как Google[30], IBM[31] и Microsoft[32] установили этические принципы, на основе которых они будут изучать применение ИИ.

Согласно принципам Google, ИИ должен быть социально выгодным; справедливым, избегать, создавать или усиливать предвзятость; построенным и протестированным для обеспечения безопасности; подотчётным людям, а также включать конфиденциальность в архитектуре системы; поддерживать высокие стандарты научного совершенства; быть доступными для использования в соответствии с этими принципами. Google также определила, что она не будет преследовать такие приложения ИИ, как «оружие или другие технологии, основная цель или реализация которых заключается в причинении или непосредственном облегчении вреда людям» или «технологии, которые собирают или используют информацию для наблюдения, нарушая международно признанные нормы».

Deepmind – исследовательская лаборатория ИИ, специализирующаяся на глубоком обучении под эгидой Google, также создала свой собственный этический консультативный орган и установила отдельные принципы и передовую практику для развития своей технологии.

Значительное развитие получило также обсуждение вопроса об ИИ в различных сферах. Например, в финансовом секторе денежно-кредитное управление Сингапура (MAS) опубликовало свои принципы поощрения справедливости, этики, подотчётности и прозрачности в использовании ИИ и аналитики данных финансового сектора в ноябре 2018 года, чтобы дать рекомендации фирмам, предлагающим финансовые продукты и услуги, по ответственному использованию ИИ и аналитики данных в целях укрепления внутреннего управления в области управления данными и их использования и, в конечном счёте, способствовать повышению доверия к использование ИИ в

---

[30] Google. Artificial Intelligence at Google: Our Principles. Retrieved from https://ai.google/principles/

[31] IBM. (2019, Jan 17). Coming soon: EU Ethics Guidelines for Artificial Intelligence. Retrieved from https://www.ibm.com/blogs/policy/ai-ethics-guidelines/

[32] Microsoft. (2020). Our approach to responsible AI. Retrieved from https://www.microsoft.com/en-us/ai/our-approach-to-ai

этом секторе.[33] Центральный банк Нидерландов (De Nederlandsche Bank) аналогичным образом опубликовал свой собственный руководящий документ в июле 2019 года, содержащий принципы ответственного использования ИИ в финансовом секторе для предотвращения любых вредных последствий для банков[34], их клиентов или ущерба репутации. Например, Королевский австралийский и новозеландский колледж радиологов предложил в августе 2019 года рамочную программу, содержащую девять этических принципов, которыми должны руководствоваться все заинтересованные стороны, участвующие в исследованиях или внедрении ИИ в медицине, включая разработчиков, руководителей медицинских служб и клиницистов[35]. В Соединённых Штатах Американская Медицинская Ассоциация также выступает за создание нормативной базы для эволюция ИИ в здравоохранении с июня 2018 года.[36]

5. Потребности и рекомендации для полиции

Принимая во внимание предшествующие правовые, социальные и этические соображения, участникам второго глобального совещания было поручено определить некоторые из наиболее насущных потребностей и рекомендовать меры, которые должны быть приняты директивными органами и межправительственными организациями для поддержки правоохранительных органов в разработке, внедрении и использовании ИИ. Ниже приводится краткое изложение собранных отзывов.

Потребности:

- Установить общий язык и исходные условия между правоохранительными органами, промышленностью, академическими

---

[33] Monetary Authority of Singapore. (2018). Principles to Promote FEAT https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/ FEAT%20Principles%20Final.pdf

[34] Van der Burgt, J. (2019). Principles for the use of Artificial Intelligence in the financial sector. De Nederlandsche Bank. https://www.dnb.nl/binaries/General%20principles%20for%20the%20use%20of%20Artificial%20InteNigence%20in%20the%20financial%20sector tcm46-385055.pdf

[35] The Royal Australian and New Zealand College of Radiologists. (2019). Ethical Principles for Artificial Intelligence in Medicine, Version 1. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2 &ved = 2ahUKEwiauKXQ1eLnAhVB3KQKHRzBDO0QFiABegQIBhAB&url=https%3A%2F%2Fwww.ranzcr.com%2Fdocuments%2F4952-ethical-principles-for-ai-in-medicine%2Ffile&usg=AOvVaw3IeDZFrKpdX0wvd Oq6cdK6

[36] Crigger, E. & Khoury, C. (2019). Making Policy on Augmented Intelligence in Health Care. AMA Journal of Ethics. https://journalofethics.ama-assn.org/article/making-policy-augmented-intelligence-health-care/2019-02

кругами и заинтересованными сторонами гражданского общества в отношении использования ИИ правоохранительными органами;

- Расширение сотрудничества между правоохранительными органами, промышленностью, академическими кругами и заинтересованными сторонами гражданского общества;
- Распространение идей относительно вариантов использования и перспектив внедрения ИИ;
- Разработка механизмов оценки использования ИИ в пилотных проектах и сотрудничество в этой области;
- Стандартизация данных, сбор данных, меры по защите данных;
- Разработать общие подходы к обезличиванию данных;
- Создание цифровых платформ для обмена знаниями, обновления проектов, анализа результатов НИОКР и возможностей финансирования.

Рекомендации

Сформулируйте заявление о принципах использования ИИ в правоохранительной деятельности, которое будет направлять правоохранительные органы для обеспечения уважения прав человека, демократии, справедливости и верховенства закона и поддерживать его в приоритете ключевых требований справедливости, подотчётности, прозрачности и лёгкости восприятия, а также безопасности и надёжности;

Разработать руководство для правоохранительных органов по внедрению новых технологий для поддержки и поощрения правоохранительных органов к изучению и инвестированию в новые ИИ, возможности развивать обучение по новым приложениям ИИ и распространять лучшие из них в практике;

- создайте базу знаний с правоохранительным сообществом о требованиях к внедрению ИИ, таких как виды проблем, которые ИИ способен решать, текущие или присущие им ограничения и ресурсы (инструменты, данные, экспертные знания, вычислительные мощности), необходимые для реализации решений ИИ;
- разработать руководство для правоохранительных органов по использованию ИИ в суде, которое оценивает влияние и результаты

конкретного использования ИИ в судах, обеспечивая при этом уважение прав человека и верховенство права;

- создать экспертно-онсультативный комитет, который будет давать рекомендации правоохранительным органам с точки зрения законодательства и служить форумом для обсуждения соответствующих законодательных актов модели с участием юридических экспертов и дру 1х ключевых заинтересованных сторон;

- определить внешний глобальный орган для оказания консультативной поддержки правоохранительным органам по этическим вопросам и оказывать поддержку в проведении аудиторских проверок для проверки того, является ли система ответственной и соответствует требованиям законодательства;

- определить внешний глобальный орган для оказания консультативной поддержки правоохранительным органам по этическим вопросам и оказывать поддержку в проведении аудиторских проверок для проверки того, является ли система ответственной и соответствует требованиям законодательства;

- интерпол и ЮНИКРИ договорились продолжать изучать потребности и рекомендации, а также опираться на них в ходе предстоящих глобальных совещаний по ИИ для правоохранительных органов.

5. Ответственный инструмент ии на службе правоохранителей

Как уже отмечалось, дискуссии об ответственном использовании ИИ все шире ведутся между государствами и во всем частном секторе. На момент подготовки проекта более 30 государств, с 2016 года приняли национальные стратегии ИИ или планы действий, большой процент которых подчёркивает важность этических соображений для использования ИИ. Кроме того, произошло несколько заметных изменений с точки зрения формулировок принципов, таких как принципы ОЭСР по ИИ, и предлагаемых этических рамок, таких как руководящие принципы Европейского Союза по этике для надёжного ИИ.

Второе глобальное совещание – это комплексный этап для правоохранительного сообщества, чтобы также принять меры, с участием представителей, подтверждающих важность ответственного ИИ. Они также чётко определили, что правоохранительные органы нуждаются в поддержке и руководстве, чтобы облегчить принятие ИИ и при этом избежать многих

ловушек. После выявления потребностей и требований правоохранительных органов и в ответ на растущее глобальное давление Интерпол и ЮНИКРИ признали, что инструментарий для ответственного внедрения ИИ в правоохранительную деятельность будет ценным вкладом с точки зрения оказания поддержки и руководства. «Инструментарий» считается предпочтительным форматом, поскольку он, отходя от существующих предлагаемых подходов «руководящих принципов», «правил» и «рамок», направлен на стимулирование позитивного потенциала ИИ в рамках правоохранительного сообщества по разработке, развёртыванию и использованию систем ИИ, обеспечивая при этом рекомендации по предотвращению любых вредных последствий. Более конкретно, это помогло бы правоохранительным органам использовать ИИ, чтобы извлечь максимальную выгоду из этой технологии законным и заслуживающим доверия образом, а не поднимать озабоченность по поводу её внедрения, что ещё больше способствовало бы созданию условий по подрыву общественного признания.

Основное внимание в этом инструментарии может быть уделено следующим вопросам:

- общее объяснение ИИ, включая соответствующее рабочее определение для правоохранительных органов;
- руководство по использованию ИИ в правоохранительных органах, включая дентификацию и компиляцию основных технологических областей и возможных вариантов использования;
- рассмотрение примеров или лучших практик надёжного, законного и ответственного использования ИИ в правоохранительных органах – обобщение важных требований, таких как справедливость, подотчётность, прозрачность и объяснимость, для рассмотрения, когда правоохранительное учреждение намеревается разработать проект с поддержкой ИИ (внутренний) или приобрести инструмент/систему ИИ (внешние решения) – и ряд рекомендуемых передовых практик, которые отражают общие принципы и направлены на укрепление доверия и социального признания;
- пошаговые рекомендации по разработке, внедрению и техническому обслуживанию усовершенствованной ИИ системы в правоохранительных органах, включая контрольный перечень оперативных соображений для обеспечения соответствия системы / операции вышеупомянутым соображениям;
- для того, чтобы добавить наибольшее значение для правоприменения, полезно подчеркнуть цель, структуру и уровень абстракции документа.

Прежде всего, как инструмент, он должен служить справочным руководством для правоохранительных органов и ни при каких обстоятельствах не должен рассматриваться как обязательный по своему характеру. Во все времена он должен быть ориентирован на практическую и оперативную деятельность и не должен впадать в концептуальные дискуссии. Нет никакой дополнительной ценности в инструменте, направленном на пересмотр устоявшихся правовых, этических и социальных дискуссий вокруг использования ИИ правоохранительными органами. Наконец, инструмент должен стремиться опираться на уже сделанную работу, и избегайте быть просто ещё одним набором руководящих принципов;

- старшие руководители полиции или ключевые лица, принимающие решения в правоохранительных органах;
- сотрудники правоохранительных органов, ответственные за инновации и использование технологий в своих соответствующих ведомствах;
- сотрудники по НИОКР, которым поручено развивать возможности ИИ внутри компании или которые могут влиять на аутсорсинговые процессы закупок;
- юристы или консультанты, которые консультируют по вопросам законов и нормативных актов, касающихся конкретного использования ИИ в полицейской работе.

В дополнение инструментарий должен быть ориентирован на представителей широкой общественности и доступен им, чтобы способствовать развитию чувства открытости и прозрачности в отношении использования ИИ правоохранительными органами и тем самым укреплять доверие общественности.

Принимая во внимание целевые аудитории, инструментарий должен стремиться поддерживать баланс в обсуждении между концептуальными, оперативными и техническими языками. Конкретные разделы могут быть разработаны для каждой из отдельных целевых аудиторий, чтобы обеспечить индивидуальные директивы для формирования и руководства каждой целевой аудиторией в соответствии с их ролью в разработке, развёртывании и использовании ответственных систем ИИ.

6. Дорожная карта

Разработка инструментария по инновациям ИИ для правоохранительных органов рекомендуется в качестве важнейшей предпосылки для дальнейшего изучения, применения и интеграции ИИ правоохранительными органами. Приняв принципиальный подход к наращиванию потенциала ИИ, правоохранительные органы могут заложить основы для обеспечения законности и общественного доверия, необходимого для социального признания.

В рамках дальнейшей деятельности по итогам второго глобального совещания по ИИ для правоохранительных органов Интерпол и ЮНИКРИ провели качественные исследования и опросы с несколькими глобальными экспертами из различных областей - правоохранительных органов, промышленности, научных кругов и других международных органов – чтобы получить надлежащую обратную связь о целесообразности этой работы и о том, как она должна быть оформлена, чтобы повысить ценность ее использования правоохранительными органами.

Разработка инструментария наряду с дальнейшим выявлением случаев использования в правоохранительных органах будет находиться в центре внимания третьего глобального совещания Интерпола – ЮНИКРИ по ИИ для правоохранительных органов в 2020 году.

Хотя Интерпол и ЮНИКРИ будут руководить разработкой инструментария, принятый подход будет носить открытый, транспарентный и основанный на широком участии характер, особенно в том, что касается уточнения принципов и требований, лежащих в основе инструментария. В этой связи настоящий доклад представляет собой открытый призыв к вовлечению заинтересованных сторон в этот процесс с тем, чтобы получить максимально полный результат.

Для дальнейшей поддержки этого процесса Интерпол и ЮНИКРИ также определили ряд соответствующих шагов, которые могли бы быть предприняты международным правоохранительным сообществом, директивными органами и межправительственными организациями для поддержки процесса обеспечения ответственного внедрения ИИ в правоохранительные органы.

К ним относятся:

- продолжение создания форума и сети координационных центров в рамках правоохранительных органов на национальном уровне в целях обмена информацией о случаях использования ИИ, опыте и практике

содействия обсуждению вопросов ответственного проектирования, развёртывания и использования ИИ правоохранительными органами;

- проведение комплексного картирования возможностей ИИ поставщиков и уровней их внедрения по ключевым правоохранительным функциям и в отношении ключевых областей преступности;
- разработка базы данных по прецедентам использования ИИ для правоохранительных органов и выявление общих черт в прецедентах использования;
- координация и сбор экспертов для обзора и анализа существующей политики, нормативных актов, законодательства, правил и процедур, имеющих отношение к использованию ИИ правоохранительными органами, а также оценка готовности к принятию ИИ;
- определение потребностей и требований для разработки программы НИОКР в области ИИ;
- организация общественных семинаров для укрепления общественного доверия и социального признания, привлечение критической обратной связи от общественности в отношении использования ИИ правоохранительными органами;
- оказание поддержки в разработке национальных правовых актов, оперативных процедур по разработке, развёртыванию и использованию ИИ и связанных с ним технических материалов для проведения национальных семинаров-практикумов в целях поддержки внедрения инструментария.

Приложение I

Терминология

Понимание возможностей и рисков ИИ может показаться непрофессионалу непреодолимым вызовом. Действительно, одной из причин возникновения неверных представлений об ИИ является непонимание этой технологии. Завеса путаницы окружает эти предметы, что отчасти объясняется их сложной технической природой, а также жаргоном и модными словечками, используемыми в связи с ИИ.

Чтобы помочь правоохранительным органам проникнуть сквозь эту завесу и прояснить некоторые концепции проблемы ИИ, некоторые термины,

упомянутые в настоящем докладе, описаны ниже. Приводятся примеры, облегчающие понимание более сложных понятий.

Однако эти описания не следует принимать за определения. Определение этих терминов выходит за рамки настоящего доклада.

Алгоритм: в информатике алгоритм – это набор инструкций, определяющих последовательность операций для выполнения вычислений, другими словами, он состоит из сценариев программирования, лежащих в основе любого программного обеспечения.

Автономная система: система, которая может выполнять запрограммированные задачи без необходимости какого-либо вмешательства человека. Существуют также полуавтономные системы, которые нуждаются в человеческом вмешательстве в какой-то момент своего функционирования.

Искусственный интеллект: подотрасль компьютерных наук, посвящённая теории и разработке компьютерных систем, способных выполнять задачи, обычно требующие человеческого интеллекта, такие как визуальное восприятие, распознавание речи, перевод между языками, принятие решений и решение проблем. В отличие от других компьютерных программ, системы ИИ не требуют явных инструкций от людей, но извлекают паттерны и изучают неявные правила из значительного числа примеров, включённых в базу данных. Приложения ИИ специализируются на выполнении одной конкретной задачи и в некоторых случаях могут даже превосходить человеческие возможности.

Большие данные: наборы данных, которые слишком велики или сложны для обработки с помощью традиционного прикладного программного обеспечения для обработки данных.

Компьютерное зрение: междисциплинарная научная область, включающая методы получения, обработки, анализа и извлечения информации из цифровых изображений или видео.

База данных: организованный набор данных, обычно хранящихся и доступных в электронном виде с помощью компьютерной системы.

Глубокое обучение: подпространство машинного обучения, которое использует искусственные нейронные сети, алгоритмы, вдохновлённые человеческим мозгом, чтобы учиться на больших объемах данных.

Алгоритмы глубокого обучения выполняют задачу многократно, каждый раз внося незначительные изменения в её внутренние характеристики для улучшения результата. Термин «глубокое обучение» возникает из нескольких (глубоких) слоёв нейронных сетей.

Deepfakes: сокращение от «глубокого обучения и подделок». Синтетический носитель информации, в котором изображения, аудио или видео людей и событий генерируются или управляются с помощью генеративных архитектур нейронных сетей. Алгоритмы Deepdale используют глубокое обучение для создания визуального и аудиоконтента, который трудно отличить от подлинного.

Распознавание лица: система, способная идентифицировать интересующих лиц по изображениям или видеозаписям утем сравнения и анализа паттернов, форм и пропорций их черт лица и контуров с лицами в базе данных.

Интернет вещей: система, которая может идентифицировать интересующих людей по изображениям или видео, сравнивая и анализируя узоры, формы и пропорции их черт лица и контуров с лицами в базе данных.

Машинное обучение: подпространство ИИ, которое использует статистические методы, чтобы дать компьютерным системам возможность «учиться» на данных, то есть постепенно повышать производительность по конкретной задаче. Алгоритмы машинного обучения не требуют явных инструкций программирования, но полагаются на шаблоны и выводы из огромного числа примеров, известных как «обучающие данные». Как только математическая модель, которая соотносит эти примеры, построена, алгоритм машинного обучения способен делать прогнозы или принимать решения о новых невидимых примерах, «тестовых данных».

Malware: сокращение от «вредоносного программного обеспечения». Вредоносное ПО – это любое программное обеспечение, намеренно созданное для нанесения ущерба или кражи данных с компьютера, сервера или компьютерной сети. Вирусы, трояны, шпионские программы и программы-вымогатели являются примерами различных видов вредоносных программ.

Обработка человеческой речи: область компьютерной лингвистики и ИИ, связанная с обработкой и анализом больших объёмов данных естественного человеческого языка. Задачи обработки естественного языка часто включают распознавание речи, понимание естественного языка, генерацию естественного языка и перевод между языками.

Нейронная сеть: базовая модель глубокого обучения. Вдохновлённые биологическими нейронами, эти алгоритмы используют несколько слоёв отдельных блоков для постепенного извлечения объектов более высокого уровня из необработанных входных данных. Например, если входные данные представляют собой изображение, то первые слои нейронной сети могут идентифицировать линии и кривые, в то время как последние слои могут идентифицировать буквы или лица.

Фишинг: мошенничество с электронной почтой или электронными коммуникациями, направленное на то, чтобы обманом заставить людей скачивать вредоносное программное обеспечение или получать конфиденциальную информацию, такую как учётные данные учётной записи или финансовая информация. Фишинговые атаки не являются персонализированными и обычно направляются массам людей одновременно. Копье – фишинг, с другой стороны, специально нацелен на жертву.

Робототехника: отрасль машиностроения, которая специализируется на разработке роботов - машин, способных выполнять сложную серию действий, которые могут управляться дистанционно или автономно. Робототехника включает в себя проектирование, конструирование, эксплуатацию и применение роботов, а также компьютерных систем для их управления, сенсорной обратной связи и обработки информации, таких как ИИ.

Распознавание речи: компьютерная программа с возможностью преобразования аудио – речи в текстовую информацию, то есть она позволяет распознавать и переводить устную речь в текст.

Контролируемое обучение: наиболее распространённая подотрасль машинного обучения, которая заключается в изучении того, как сопоставить входные данные с выходной меткой, основана на ряде примеров пар вход – выход. Для определённого количества входных признаков (например, фрукт, красный, круглый) предусмотрена метка (например, яблоко). С помощью алгоритмов машинного обучения обучающий набор данных используется для построения математической модели, позволяющей прогнозировать классификацию немеченых данных.

Неконтролируемое обучение: задача машинного обучения, которая находит закономерности в данных, которые не были помечены или классифицированы. Он может быть использован для кластерного анализа, который состоит из группировки элементов данных с аналогичными признаками.

Приложение II

Список аббревиатур

АПР	Автоматизированное Принятие Решений
AFP	Австралийская федеральная полиция
ИИ	Искусственный интеллект

ГЭВУ-ИИ	Группа экспертов высокого уровня по искусственному интеллекту
ИИ-ОПиОБ	Искусственный интеллект для обеспечения правопорядка и общественной безопасности
СВН	Система видеонаблюдения
ЕС	Европейский Союз
СОПД	Справедливость, ответственность, прозрачность и доходчивость
ОБЗД	Общие Правила Защиты Данных
GPS	Система глобального позиционирования
ИЦИ	Инновационный центр Интерпола
СВУ	Самодельное взрывное устройство
ГИКИ	Глобальный инновационный комплекс Интерпола
ИНТЕРПОЛ	Международной организации уголовной полиции
ДПО	Директива по правоохранительным органам 2016/680
ДКУС	Денежно-кредитное управление Сингапура
ОЧР	Обработка человеческой речи
non-POI	Личность не представляющая интерес
НПАЯ	Национальное полицейское агентство Японии
ОЭСР	Организация экономического сотрудничества и развития
ИиР	Исследования и разработки
БПЛА	Беспилотный летательный аппарат (дрон)
ЮНИКРИ	Межрегиональный Научно-исследовательский институт Организации Объединённых Наций по вопросам преступности и правосудия
ЦУИТСБ	Центральное управление информационных технологий в секторе безопасности

Про Интерпол

Интерпол – крупнейшая в мире международная полицейская организация.

Её роль заключается в оказании помощи правоохранительным органам 194 стран – членов в борьбе со всеми формами транснациональной преступности. Интерпол работает над тем, чтобы помочь полиции всего мира справиться с растущими угрозами преступности в 21 веке, предоставляя высокотехнологичную инфраструктуру технической и оперативной поддержки.

Её услуги включают в себя целевую подготовку, экспертную следственную поддержку, специализированные базы данных и защищённые полицейские каналы связи.

Расположенный в Сингапуре, в рамках Глобального инновационного комплекса Интерпола (IGCI), инновационный центр Интерпола (IC) работает над созданием стратегических партнёрств с правоохранительными органами, академическими кругами и частным сектором на глобальном, региональном и национальном уровнях. Это сотрудничество помогает Интерполу в разработке инновационных решений для борьбы с новейшими угрозами.

Про Юникри

Межрегиональный Научно-исследовательский институт Организации Объединённых Наций по вопросам преступности и правосудия был создан в

1968 году. В рамках широкого круга своих полномочий институт вносит вклад посредством проведения научных исследований, подготовки кадров, сбора, обмена и распространения информации, в разработку и осуществление более эффективной политики в области предупреждения преступности, правосудия и новых угроз безопасности, уделяя должное внимание интеграции такой политики в более широкую политику социально-экономических преобразований и развития, а также защите прав человека.

В 2017 году ЮНИКРИ открыл свой центр искусственного интеллекта и робототехники в Гааге, Нидерланды, с целью углубления понимания искусственного интеллекта, робототехники и связанных с ними технологий в области предупреждения преступности, уголовного правосудия, верховенства права и безопасности. Центр стремится обмениваться знаниями и информацией о потенциально полезном применении технологий и вносит свой вклад в борьбу с любыми вредными явлениями и современными угрозами.

Искусственный интеллект и правоохранительные органы

STUDY

Requested by the LIBE committee



Artificial Intelligence and Law Enforcement

Impact on Fundamental Rights

Влияние на основные права

Департамент политики по правам граждан и конституционным вопросам, Главное управление внутренней политики, июль 2020.

Этот документ был запрошен Комитетом Европейского парламента по гражданским свободам, правосудию и внутренним делам.

АВТОР проф. Д-р Глория ГОНСАЛЕС ФУСТЕР, Брюссельский университет (VUB)

ОТВЕТСТВЕННЫЙ АДМИНИСТРАТОР Алессандро ДАВОЛИ

ПОМОЩНИК РЕДАКЦИИ Гинка ЦОНЕВА

ЯЗЫКОВЫЕ ВЕРСИИ Оригинал: EN

О редакторе

Политические департаменты предоставляют внутренних и внешних экспертов для поддержки комитетов Европарламента и других парламентских органов в формировании законодательства и демократическом контроле над внутренней политикой ЕС.

Чтобы связаться с отделом политики или подписаться на обновления, напишите по адресу: Департамент политики по правам граждан и конституционным вопросам Европейский парламент B-1047 Брюссель, электронная почта: poldep-citizens@europarl.europa.eu. Рукопись завершена в июле 2020 г. © Европейский Союз, 2020

Этот документ доступен в Интернете по адресу: http://www.europarl.europa.eu/supporting-analyses

Отказ от ответственности и авторские права

Мнения, выраженные в этом документе, являются исключительной ответственностью авторов и не обязательно отражают официальную позицию Европейского парламента.

Воспроизведение и перевод в некоммерческих целях, разрешается при условии указания источника.

Список сокращений

ACLU	Американский союз гражданских свобод
ADM	Автоматизированное принятие решений
ИИ	Искусственный интеллект
CJEU	Суд Европейского Союза
DAPIX	Рабочая группа по обмену информацией и защите данных
DPA	Data Protection Authority
EASO	Европейское бюро поддержки Asylum
ЕС	Европейская комиссия
ЕСПЧ	Европейская конвенция о правах человека
ECRIS-TCN	Европейская система информации о судимости для граждан третьих стран
ЕСПЧ	Европейский суд по правам человека
EDPB	Европейский совет по защите данных
EDPS	Европейский супервайзер по защите данных
EDRI	Европейская инициатива в области цифровых прав
EES	Система входа / выхода
EIO	Европейский приказ о расследовании
EPIC	Электронный информационный центр конфиденциальности
ЕОКЗР	Европейская прокуратура
ЕС	Европейский Союз
FAT	Справедливость, подотчетность и прозрачность
FIU	Группа финансовой разведки
GDPR	Общий регламент по защите данных
GSMA	Ассоциация Global System for Mobile Communications
GVM	Матрица насилия в бандах
ICO	Офис комиссара по информации
IT	Информационные технологии

JRC	Объединенный исследовательский центр
LED	Директива по обеспечению соблюдения законов
LFR	Живое распознавание лиц
OECD	Организация экономического сотрудничества и развития
PNR	Запись имени пассажира
RBI	Удаленная биометрическая идентификация
SIS	Шенгенская информационная система
UNICRI	Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия
VIS	Визовая информационная система

Введение

Искусственный интеллект (ИИ) занимает важное место в повестке дня Европейского Союза (ЕС). Дискуссии о его возможном регулировании стали особенно заметными после того, как Урсула фон дер Ляйен заявила еще до своего назначения на пост президента Европейской комиссии (ЕК) о твердом намерении поместить ИИ в число главных приоритетов Комиссии. Утверждение ИИ в качестве приоритета политики на уровне ЕС сопровождалось размышлениями о том, как укрепить доверие к технологиям ИИ и как гарантировать, что системы ИИ не нарушают при разработке или развертывании фундаментальные права ЕС. Это конкретное размышление на самом деле не является полностью новым, но оно укоренилось в предыдущих юридических и политических дебатах по вопросам основных прав, связанных, в частности, с «большими данными», а также, в более общем плане, связанных с регулированием обработки как личных, так и неличных данных.

Цель:

Это исследование направлено на анализ воздействия ИИ на основные права ЕС в области правоохранительной деятельности и правосудия. Оно подходит к предмету с точки зрения законодательства и политики ЕС. Сначала в нем кратко представлены основные характеристики применимой правовой

базы. Во- вторых, он вводит в последнее время и текущих событий в этой области, сосредоточив внимание на «предсказательной полиции», распознавание лиц с использованим ИИ. В нём обсуждается влияние этих тенденций на основные права и рассматриваются соответствующие политические дискуссии, касающиеся регулирования ИИ. После такого исследования в исследовании предлагаются некоторые конкретные рекомендации.

Выводы:

Сфера правоприменения и уголовного правосудия особенно чувствительна, поскольку затрагивает ключевые вопросы взаимоотношений между человеком и государством. Существует широкий консенсус в отношении того факта, что использование систем искусственного интеллекта в этой области может существенно повлиять на основные права ЕС и, в целом, на саму демократию. Таким образом, этот вопрос заслуживает особого рассмотрения в контексте любой дискуссии о будущем надежного ИИ.

Обучение:

- показывает, что появление ИИ в области правоохранительной деятельности уже стало реальностью, поскольку системы ИИ все чаще применяются; такие системы могут принимать самые разные формы и возникать на перекрестке различных устойчивых тенденций для увеличения использования данных, алгоритмов и вычислительной мощности; эти изменения связаны с ранее существовавшими тенденциями, некоторые из которых ранее широко рассматривались в рамках других понятий или политических приоритетов («большие данные»);
- документы, подтверждающие, что такие разработки уже вызвали серьезные разногласия, особенно в отношении «прогнозирующей полицейской деятельности», распознавания лиц, ИИ, а также ИИ-анализ и границы (включая отражение Европейской системы информации и разрешений для путешествий, ETIAS), например, в судебных процессах и призывах гражданского общества лучше предотвращать или снижать связанные риски как в ЕС, так и за его пределами;
- указывает на то, что дискуссии о регулировании ИИ в ЕС глубоко укоренились в повестке дня единого цифрового рынка ЕС, и что в целом,

хотя они могут относиться к необходимости учитывать особенности правоохранительных органов и уголовного правосудия, такие политические обсуждения чаще всего не проводятся на основе подробного анализа и с учетом конкретных применимых правил (и особенно, применимых ограничений и отступлений);

- предупреждает, что такие политические дискуссии страдают от стойкого двойственного отношения к роли «этики» в отношении защиты основных прав, порождая не только отсутствие концептуальной точности, но, что наиболее важно, неопределенность в отношении того, будет ли обеспечена эффективная защита основных прав;
- подчеркивает, что действующая правовая база ЕС по защите данных не предполагает надежных гарантий для отдельных лиц в свете все более широкого использования автоматизированного принятия решений и профилирования в правоохранительных целях и в целях уголовного правосудия, такие как:
- общие меры предосторожности, предусмотренные Общим регламентом защиты данных (GDPR) - не обязательно применяются, когда обработка выполняется для таких целей, поскольку могут применяться ограничения и отступления;
- директива о защите данных правоохранительных органов (Директива LED), которая может быть применимыми соответствующими инструментами, обеспечивает гарантии, аналогичные гарантиям GDPR, но, тем не менее, не полностью эквивалентные, и в равной степени предусматривает возможные ограничения и отступления.
- рассматривает различные аспекты основных прав, связанных с ИИ, в области правоохранительной деятельности и уголовного правосудия, демонстрируя тот факт, что они включают вопросы конфиденциальности и защиты данных, а также другие проблемы, в частности, связанные с недискриминацией;
- описывает проблематичное отсутствие минимальных стандартов прозрачности в отношении поддержки исследований ИИ за счет средств ЕС, что, в частности, влияет на возможность оценки соответствия финансируемых исследований соблюдению основных прав ЕС и законодательства ЕС в целом, а также дальнейшую научную работу в направлении надежные ИИ-решения;
- предупреждения о том, что ответные меры на вспышку Covid-19 привели к быстрому распространению технологических мер и инициатив, основанных на данных, которые требуют тщательной оценки, в том числе инициатив, которые имеют целью поддержание беспрецедентно широко распространенного обобщенного сбора данных об отдельных лицах («контакт отслеживание приложений») и инициативы, основанные на хрупком различии между «личными» и «анонимными» данными для

облегчения обширной обработки данных;

- рекомендует уделить должное внимание необходимости законодательного вмешательства для гарантии основных прав ЕС в области правоохранительной деятельности и уголовного правосудия; что любая возможная роль, отводимая «этике» в таком вмешательстве, должна быть подробно разъяснена и обоснована; что возможные пробелы и неэффективность закона о защите данных ЕС, а также национальных законов, реализующих закон о защите данных ЕС, должны быть должным образом изучены, особенно в свете правоохранительной деятельности и контекста уголовного правосудия; что финансируемые ЕС исследования искусственного интеллекта должны быть лучше сформулированы, и, наконец, что события, связанные со вспышкой Covid-19, должны отслеживаться с особенным вниманием.

Общая информация

Ключевые результаты

Правоохранительные органы и следствие могут извлечь выгоду из ИИ и связанных систем и технологий, будучи принятами, и разработанами для правоохранительных органов и следствия в Европейском союзе (ЕС).

Однако некоторые из этих решений вызывают важные вопросы с точки зрения их совместимости с основными правами ЕС.

Политические дискуссии на уровне ЕС по регулированию ИИ до недавнего времени были отмечены их сильной интеграцией в развитие единого цифрового рынка. В этом политическом контексте Европейская комиссия (ЕК), в частности, выступает за внедрение ИИ, в то же время, преследуя цель создания «экосистемы доверия» – доверия к ИИ – как самостоятельной политической цели. Этические соображения дали много внимания с этой точки зрения.

Однако масштабы и серьезность проблем, создаваемых ИИ в области правоохранительной деятельности, не могут быть легко решены размышлениями. В этом смысле будущие шаги должны, в частности, учитывать правовые особенности данной области и, в первую очередь, сложности и ограничения правовой базы ЕС по защите данных, особенно в том, что касается обработки персональных данных для целей правоохранительных органов и уголовного правосудия, и в более общем плане в отношении обработки данных в сфере свободы, безопасности и правосудия (AFSJ).

Вспышка Covid-19 привела к тому, что решения на основе данных и искусственного интеллекта стали более распространенными, чем когда-либо, потенциально экспоненциально увеличивая количество личных данных, которые в конечном итоге станут доступны для правоохранительных органов. В то время как гарантии основных прав, включая гарантии защиты данных, сейчас кажутся более важными, чем когда-либо, были также случаи, когда этим гарантиям угрожали исключительные меры, принятые в связи с потребностями, связанными с кризисом. Это создает особенно щекотливую ситуацию для основных прав ЕС, требующую большой бдительности.

Искусственный интеллект (ИИ) может найти существенное применение в области правоохранительной. Эта идея широко принимается и одобряется на уровне Европейского союза (ЕС)[37], и тенденция к использованию автоматизированных методов обработки и алгоритмов в предупреждении преступности и системах уголовного правосудия описывается как в целом растущая уже в течение ряда лет (MSI-NET, 2018, 10).

Как ни парадоксально, несмотря на широкое признание этой напряженности, существует относительно мало исследований или даже политических дискуссий по конкретным потребностям и проблемам регулирования на уровне Европейского союза (ЕС) ИИ в правоохранительной и уголовной юстиции. Эти возможные специфические потребности и проблемы часто появляются в качестве заключительной мысли, если не в последнюю очередь, среди более широких размышлений, связанных с регулированием ИИ в целом. Почти как исключение из этого правила, Европейский парламент в настоящее время обсуждает проект отчета об искусственном интеллекте в уголовном праве и его использовании полицией и судебными органами в уголовных делах (LIBE, 2020/2016 (INI)).

На уровне ЕС обсуждения возможной потребности в нормативной базе ИИ в основном всплыли на поверхность и до сих пор развивались в контексте единого цифрового рынка. Это не без последствий для характера и существа дебатов и, в частности, имеет тенденцию упускать из виду уникальность правоохранительной деятельности и уголовного правосудия, как в отношении конкретных рисков в этой области, так и особенностей правовой базы ЕС в Зоне свободы, безопасности и правосудия (AFSJ).

Если политические дебаты на уровне ЕС лишь ограниченно затронули проблемы ИИ в правоохранительной деятельности и уголовном правосудии, многие из этих проблем, тем не менее, уже явно всплывают, часто вызывая споры, на территории ЕС и во всем мире. Это, скорее всего, связано с тем, что

---

[37] «Alcan ... помогает обнаруживать мошенничество и угрозы кибербезопасности и позволяет правоохранительным органам более эффективно бороться с преступностью» (COM (2019) 168 финал, 1).

правоохранительные органы и уголовное правосудие имеют отношение к фундаментальным аспектам отношений между отдельными лицами и государством, отношения, которые, таким образом, особенно чувствительны к глубоким преобразованиям потенциально перемещаемых систем искусственного интеллекта. Однако может также случиться так, что способ развертывания определенных связанных технологий был не самым подходящим, и что различные подходы – и, возможно, действительно, пересмотренная нормативно-правовая база – способствовали бы снижению рисков основных прав, облегчению критических проблем, и повысить доверие к этим технологиям.

Европейская комиссия уже в 2014 году отметила, что, хотя оцифровка государственных услуг открыла новые возможности для оптимизации анализа данных, «сообщаемое использование аналогичных технологий для целей наблюдения государственными или частными субъектами может вызвать обеспокоенность и снизить доверие к цифровым технологиям, экономия среди частных лиц и организаций», заслуживающая особого внимания (COM (2014) 442 final, 3). По мнению некоторых наблюдателей, усиление повсеместного наблюдения является одним из последствий появления ИИ в некоторых странах, таких как США и Китай (ИИ Now Institute, 2018).

Много было сказано о «гонке за господство ИИ» или «гонке ИИ», обычно имея в виду способность конкретных субъектов использовать экономические преимущества разработок ИИ[38]. В контексте правоохранительной деятельности и уголовного правосудия наиболее важной продолжающейся гонкой может быть гонка между законодательными усилиями по надлежащему определению и противодействию рискам, вызываемым ИИ, с одной стороны, а также судебные разбирательства и другие события «снизу вверх», которые выдвигают на передний план ряд фундаментальных вопросов, которые, как представляется, требуют если не дополнительной защиты со стороны закона, то, по крайней мере, срочно, большей ясности[39].

1.1. Цели и структура

Это исследование направлено на критическую оценку текущих событий в отношении ИИ в области правоохранительной деятельности и уголовного правосудия, чтобы проанализировать их влияние на основные права ЕС и, на основе такой оценки, выдвинуть политические рекомендации. Для этого

[38] См., Например: Castro, McLaughlin & Chivot, 2019.
[39] В отношении этого «соревнования» и регулирования распознавания лиц см., Например: Lynch, 2020.

сначала кратко представлена соответствующая правовая база, а затем рассматриваются основные тенденции и противоречия в этой области, уделяя особое внимание «прогнозирующей полицейской деятельности», распознаванию лиц, ИИ и уголовному правосудию, а также ИИ и пограничному контролю. Затем он анализирует их влияние на основные права ЕС, прежде чем перейти к соответствующим политическим обсуждениям, касающимся регулирования ИИ, в разделе, также исследующем поддержку ИИ в правоохранительной деятельности и уголовном правосудии за счет финансирования ЕС. В исследовании также представлены некоторые основные важные события, произошедшие после вспышки вируса Covid-19. В заключение предлагается ряд рекомендаций в отношении политики.

Понятие ИИ здесь понимается в широком смысле, чтобы предложить широкий обзор соответствующих дебатов и проблем. Юридические и политические дискуссии часто имеют тенденцию смягчать границы между определенными сопутствующими понятиями, а вопросы, которые представляют интерес для целей обсуждения ИИ в области правоохранительной деятельности и уголовного правосудия, иногда проявляются в зависимости от другой терминологии (например, в дебаты вокруг «алгоритмической дискриминации», «подотчетных алгоритмов», «алгоритмической прозрачности» и т. д.).

Исследование не преследует цели исчерпывающего охвата всех недавних и текущих событий в этой области, которых много. В этом смысле Агентство ЕС по основным правам составило сборник из почти 300 политических инициатив в государствах-членах ЕС и за его пределами на период 2016-2020 гг. (EU FRA, апрель 2020 г.).

Исследователи, работающие над регулированием ИИ, также подчеркнули сложность полного обзора многих инициатив, касающихся этических, социальных и правовых аспектов ИИ (Boddington, 2017, 3).

Исследование также не затрагивает такие вопросы, как неправомерное использование ИИ в преступных целях. Когда ИИ используется злонамеренно (Brundage, 2018), могут возникнуть дополнительные проблемы с соблюдением основных прав.

1.2. Методология

Исследование основано на кабинетных исследованиях и обзоре существующих доступных данных, исследованиях и анализах из источников и документов из ЕС, национальных и международных организаций, а также

органов по защите данных (DPA), экспертов, академических кругов, промышленности и гражданского общества. Он в основном включает правовые инструменты и программные документы институтов, органов и агентств ЕС, а также Совета Европы. Анализ первичного и вторичного законодательства ЕС составляет важную часть исследования. Различные отчеты также использовались в той мере, в какой они полезны для иллюстрации последних тенденций и противоречий.

2. Правовая основа ЕС

Прежде чем рассматривать влияние ИИ на основные права в области правоохранительной деятельности и уголовного правосудия, полезно вкратце напомнить, какие стандарты применяются в ЕС. В этом разделе кратко рассматриваются основные элементы соответствующей правовой базы ЕС, затрагивая как первичное, так и вторичное право.

На самом деле существует множество правовых инструментов, которые можно рассматривать как прямо или косвенно применимые к разработкам, связанным с искусственным интеллектом.[40] Для целей этого исследования особое внимание здесь должно быть уделено обязательствам ЕС по основным правам, а также правилам в отношении данных и их свободному использованию движение в свете важности данных как инструмента, способствующего развитию ИИ, и как его продукта.

Важно помнить, однако, что обязательства ЕС права сосуществовать с другими основными правами и обязанностями по защите данных, таких как производные от национальных правовых систем. Кроме того, особого упоминания заслуживают инструменты Совета Европы, в первую очередь Европейская конвенция о правах человека (ЕКПЧ) и Конвенция о защите частных лиц в отношении автоматической обработки персональных данных («Конвенция 108»)[41], которая недавно была пересмотрена, привело к модернизированной версии, известной как «Конвенция 108+»[42].

Эти инструменты Совета Европы сопровождаются инструментами мягкого права, такими как Руководящие принципы по искусственному интеллекту и защите данных, опубликованные Консультативным комитетом Конвенции № 108 в 2019 году[43]. Ранее, в 2018 году, Консультативный комитет

---

[40] Как, например, закон ЕС о кибербезопасности (Hamon, Junklewitz & Sanchez, 2020, 4).

[41] Конвенция о защите частных лиц при автоматической обработке персональных данных, ETS № 108.

[42] См. Протокол о внесении изменений в Конвенцию о защите частных лиц в отношении автоматической обработки персональных данных, CETS № 223.

[43] Консультативный комитет Конвенции о защите физических лиц при автоматизированной обработке

Конвенции № 108 также принял Практическое руководство по Использование личных данных в секторе полиции, предлагающее руководство о том, как законно предотвращать преступность и бороться с ней, в том числе посредством использования личных данных (Консультативный комитет Конвенции 108, 2018 г.).

Руководство предупреждает, что существуют «значительные риски», связанные с использованием технологий больших данных и методов анализа для помощи в раскрытии преступлений, и определяет ряд требований, на которые контролерам данных рекомендуется «обращать дополнительное внимание» при обработке персональных данных для таких целей, такие как особые требования к осведомленности (там же, 10-11).

2.1. Основной закон

Как установлено в статье 2 Договора о ЕС, ЕС «основан на ценностях уважения человеческого достоинства, свободы, демократии, равенства, верховенства закона и уважения прав человека, включая права лиц, принадлежащих к меньшинствам». Статья 6 Договора ЕС определяет, какие основные права признаются в качестве таковых законодательством ЕС, со ссылкой на будущее присоединение к Европейской конвенции о правах человека (ЕКПЧ), основные права, которые являются частью общих принципов права ЕС и основные права, признанные в Хартии основных прав ЕС, такие как человеческое достоинство (статья 1), право на жизнь (статья 2), право на неприкосновенность личности (статья 3), право на свободу и безопасность (статья 6), право на уважение частной и семейной жизни (статья 7), право на защиту личных данных (статья 8), свободу слова и информации (статья 11), свободу собраний и ассоциация (статья 12), равенство перед законом (статья 20), недискриминация (Статья 21), права ребенка (статья 24), право на эффективное средство правовой защиты и справедливое судебное разбирательство (статья 47), а также презумпцию невиновности и право на защиту (статья 48).

Все эти основные права применимы также в отношении правоохранительных органов и уголовного правосудия; требования основных прав, вытекающие из основного закона, применяются ко всем областям права ЕС. В отношении права на защиту личных данных, закрепленного в статье 8, следует отметить, что Декларация о защите личных данных в области

в Персональные данные (Конвенция 108), Руководящие принципы по искусственному интеллекту и защите данных,
T-PD (2019) 01.

сотрудничества судебных органов по уголовным делам и сотрудничества полиции, приложенная к Лиссабонскому договору, гласит, что «особые правила о защите личных данных и свободном перемещении таких данных в сферах судебного сотрудничества по уголовным делам и сотрудничества полиции на основании статьи 16 Договора о функционировании Европейского Союза, может оказаться необходимым из-за специфического характера этих сфер»[44].

2.2. Вторичное право

В этом разделе представлены наиболее важные элементы вторичного права ЕС, применимые к обработке как личных, так и неличных данных. Различие между личными и неличными данными не лишено трений, особенно потому, что технологические разработки, в том числе разработки, связанные с ИИ, могут обязывать рассматривать как личные данные определенные наборы данных, которые ранее не считались таковыми.

2.2.1. Правила обработки персональных данных

Личные данные определяются в законодательстве ЕС как «любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу («субъекту данных»); идентифицируемое физическое лицо – это лицо, которое может быть идентифицировано напрямую или косвенно, в частности, посредством ссылки на идентификатор, такой как имя, идентификационный номер, данные о местоположении, сетевой идентификатор, или на один или несколько факторов, специфичных для физической, физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого природного человек»[45].

Право на защиту личных данных в настоящее время признано фундаментальным правом ЕС как в Хартии основных прав ЕС (статья 8), так и в договорах (статья 16 Договора о функционировании ЕС). Это право в настоящее время признано автономным фундаментальным правом, отличным от права на уважение частной жизни, с которым оно исторически было тесно связано в некоторых правовых системах. Однако это не означает, что такое право не служит одновременно другим основным правам, включая право на

---

[44] Декларация 21 деклараций, приложенных к Заключительному акту Межправительственной конференции, принявшей Лиссабонский договор, подписанной 13 декабря 2007 г.

[45] Статья 4 (1) Общего регламента по защите данных (GDPR).

уважение частной жизни. В этом смысле вторичный закон ЕС, подкрепляющий статью 8 Хартии ЕС, одновременно направлен на обеспечение соблюдения всех основных прав[46].

Правовая база ЕС по защите данных состоит из ряда различных правовых инструментов, из которых необходимо упомянуть:

- регламент (ЕС) 2016/679[47], или Общий регламент по защите данных (GDPR), названный «общим», потому что он применяется «в целом» к обработке персональных данных в пределах его материала и территориальный охват (но не относится к обработке персональных данных учреждениями, органами, офисами и агентствами ЕС);
- директива (ЕС) 2016 / 680[48], известная как Директива об охране правопорядка (LED), которая в целом применяется к обработке персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или судебного преследования уголовных преступлений или исполнения уголовных наказаний, но только тогда, когда эти органы обрабатывают персональные данные для таких целей (но не распространяется на обработку персональных данных учреждениями, органами, офисами и агентствами ЕС);
- регламент (ЕС) 201 8/1 725[49], или EU-DPR, который обычно применяется к обработке личные данные учреждениями, органами, офисами и агентствами ЕС, но включают специальные правила для обработки «оперативных личных данных»[50], например, Евроюстом, и не входит в сферу ее компетенции Европол и Европейская прокуратура до

---

[46] Это имеет практическое значение для толкования GDPR. В его статье 35, например, говорится о необходимости учитывать вероятный высокий риск «для прав и свобод человека». Это было интерпретировано как в первую очередь касающееся права на защиту данных и неприкосновенность частной жизни, но также потенциально затрагивающие другие основные права, такие как свобода слова, свобода мысли, свобода передвижения, запрет дискриминации, право на свободу, совесть и религию (статья 29 WP, WP 248 rev. 01, 6).

[47] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите природных лиц в отношении обработки персональных данных и свободного перемещения таких данных, а также отмены Директивы 95/46 / ЕС (Общие правила защиты данных) (текст, имеющий отношение к ЕЭЗ), OJL 119, 4.5.2016, стр. 1-88.

[48] Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовные преступления или исполнение уголовных наказаний, а также о свободном перемещении таких данных, а также об отмене Рамочного решения Совета 2008/977 / JHA [2016] OJL 119/89, с. 89-131.

[49] Регламент (EU) 2018/1725 Европейского парламента и Совета от 23 октября 2018 года о защите физических лиц в отношении обработки персональных данных учреждениями, органами, офисами и агентствами Союза и о свободном перемещении такие данные и отменяющий Регламент (ЕС) № 45/2001 и Решение № 1247/2002 / ЕС, OJL
295, 21.11.2018, стр. 39-98.

[50] «Оперативные персональные данные» - это все персональные данные, обрабатываемые органами, офисами или агентствами ЕС при выполнении действий, которые подпадают под действие Главы 4 (Судебное сотрудничество по уголовным делам) или Главы 5 (Сотрудничество полиции) Раздела V Части Три TFEU для достижения целей и задач, изложенных в правовых актах, учреждающих эти органы, офисы или агентства (статья 3 (2) Регламента (ЕС) 2018/1725).

возможных изменений в 2022 году;

директива 2002/58/ЕС[51], или Директива об электронной конфиденциальности, применяемая к обработке персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи общего пользования.

Помимо таких инструментов, другие правовые инструменты включают особенно важные правила защиты данных, применяемые к конкретным действиям по обработке данных в этой области, такие как, например:

- регламент (ЕС) 2016/794[52], или Регламент Европола об Агентстве ЕС по сотрудничеству в правоохранительной сфере (Европол) - считается «центром обмена информацией в Союзе»[53], в котором есть свои собственные положения о защите данных;
- постановление Совета (ЕС) 201 7/1939[54], Постановления ЕОКЗР о Европейской прокуратуре, который также имеет собственные положения о защите данных;
- регламент (ЕС) 2018/1727[55], или Регламент Евроюста об Агентстве Европейского союза по сотрудничеству в области уголовного правосудия (Евроюст), в котором есть правила защиты данных, которые следует рассматривать как специальный закон для соответствующих положений Регламента EU-DP;

Панорама закона ЕС о защите данных на самом деле более сложна, чем можно предположить из этой короткой презентации. Даже если создание «согласованной основы для всей деятельности правоохранительных органов по обработке данных в правоохранительных целях было серьезной, повторяющейся проблемой Европейского парламента в течение многих лет (EP, 2014, 15), законодательство ЕС в настоящее время не предлагают полностью однородный вид. Подход, особо закрепленный LED в сочетании с EU-DPR, в соответствии с которым определенные агентства ЕС, обрабатывающие данные в правоохранительных целях, исключаются из сферы действия общих

---

[51] Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г., касающаяся обработки личных данных и защиты конфиденциальности в услугах электронных коммуникаций (Директива о конфиденциальности
и электронных коммуникациях), OJL 201, 31.7. 2002, стр. 37-47 с последующими поправками.

[52] Регламент (ЕС) 2016/794 Европейского парламента и Совета от 11 мая 2016 года об Агентстве Европейского Союза по сотрудничеству в правоохранительной сфере (Европол) и заменяющий и отменяющий решения Совета 2009/371 / JHA, 2009/934 / JHA, 2009/935 / JHA, 2009/936 / JHA и 2009/968 / JHA, OJL 135, 24.5.2016, стр. 53-114.

[53] Регламент (ЕС) 2016/794 Европейского парламента и Совета от 11 мая 2016 года об Агентстве Европейского союза по сотрудничеству в правоохранительной сфере (Европол) и заменяющий и отменяющий решения Совета 2009/3 71 / JHA, 2009/934 / JHA, 2009/935/JHA, 2009/936/JHA и 2009/968/JHA, OJL 135, 24.5.2016, стр. 53-114.

[54] Постановление Совета (EU) 2017/1939 от 12 октября 2017 г. о расширении сотрудничества по созданию Европейская государственная прокуратура («ЕППО»), OJL 283, 31.10.2017, стр. 1 -71.

[55] Сольный концерт (12) из (ЕС) 2016/794.

положений в этой области, был описан как ведущий к многоуровневой защите данных режим, в котором применяются разные правовые инструменты и, следовательно, разные стандарты, влияющие на людей при осуществлении их прав на защиту данных» (Belfiore, 2013, 367). Существует также ряд конкретных положений о защите личных данных в некоторых инструментах ЕС, которые остались незатронутыми вступлением в силу LED и с тех пор не были пересмотрены - особые положения о защите личных данных, которые вступили в силу ранее. Май 2016 г. в области судебного сотрудничества по уголовным делам и сотрудничества полиции. В июне 2020 года Европейская комиссия объявила о своем плане действий по постепенному согласованию с LED положений, все еще требующих согласования, всего 10, согласно ее оценке (COM (2020) 262 final).

Часто дискуссии о возможной необходимости будущего регулирования ИИ на уровне ЕС принимают в качестве отправной точки явное или неявное предположение, согласно которому общие стандарты GDPR являются центральным элементом действующей правовой базы, если не единственным элементом, который находится на рассмотрении (Пеннер, 2019). Однако, при сосредоточении внимания на обработке персональных данных для правоохранительных органов и уголовного правосудия такая отправная точка не подходит по двум основным причинам:

- во-первых, GDPR может во многих соответствующих случаях не применяться, поскольку будут применяться другие инструменты;
- во-вторых, даже если GDPR действительно применяется, могут применяться ограничения, основанные на том факте, что обработка связана с правоохранительными органами и уголовным правосудием, де-факто изменяя общие гарантии, которые он предусматривает.

Таким образом, крайне важно правильно расположить обсуждения регулирования ИИ в этой области, основывая их на более точном понимании применимых правил. В приложении к этому исследованию представлен обзор некоторых из наиболее важных положений GDPR и LED в отношении алгоритмической обработки данных, демонстрируя, что они не являются полностью случайными.

Как пояснил Европейский надзорный орган по защите данных (EDPS), в области правоохранительных органов «используемые действия по обработке данных часто вызывают недоумение для отдельных лиц, из-за чего им трудно узнать, кто и для каких целей обрабатывает их данные», и Права людей часто ограничиваются, несмотря на то, что «влияние обработки данных на их права и свободы является значительным» (EDPS, 2019, 38).

Дополнительной проблемой с точки зрения субъекта данных является тот факт, что к некоторым действиям по обработке данных могут применяться сложные комбинации различных положений. В зависимости от точной цели каждой операции обработки и личности контролера[56]. В AFSJ тот факт, что данные деятельность по обработке, относящаяся к некоторым информационным системам, регулируется «сложными режимами защиты данных из-за их множественного возможного использования», что может привести к проблемной неясности (FGB, 2019, 4).

Вопрос о том, предлагает ли GDPR как таковой надлежащую защиту для людей перед лицом распространения автоматизированного принятия решений, сам по себе не решен (Penner, 2019). Что касается гарантий, полезных в контексте ИИ часто цитируемым положением GDPR является его статья 22, посвященная «автоматизированному индивидуальному принятию решений, включая профилирование»[57]. Многие, включая Европейскую комиссию, конкретно ссылаются на статью 22 GDPR, когда учитывая будущее ИИ в Европе (COM (2019) 168 final, 4).

Однако существует много разногласий относительно точной сферы действия статьи 22 GDPR и самой ее природы - вводит ли она общий запрет на определенные типы автоматизированных решений или предоставляет ли она субъектам данных некоторые права, независимо от того, какие типы автоматизированных решений взяты (Brkan, 2019, 98; A29WP, 2017/2018,19).

Также существуют разногласия по поводу правовых последствий статьи 22 GDPR. Наконец, существуют разногласия по поводу того, действительно ли данное положение полезно на практике - насколько эффективно оно применяется. Существование «права на объяснение» в соответствии с GDPR также широко обсуждалось, что привело, например, к утверждению, что правовая основа для такого права является «довольно шаткой и неубедительной» (Temme, 2017, 482).

Эти проблемы вызвали то, что некоторые называют «обширными дебатами в исследовательском сообществе», переплетенными с столь же обширными дебатами о самой объяснимости систем ИИ (Sartor and Lagioia, 2020, 54).

Во всех случаях, когда применяются некоторые из упомянутых инструментов, тот факт, что определенные операции по обработке данных

---

[56] См. описанный ниже пример Европейской системы информации и разрешений на поездки (ETIAS).

[57] Профилирование определяется в статье 4 (4) GDPR как «любая форма автоматизированной обработки личных данных, состоящая из использования личных данных для оценки определенных личных аспектов, связанных
с физическим лицом, в частности, для анализа или прогнозирования аспектов, касающихся этого, производительность физического лица на работе, экономическое положение, здоровье, личные предпочтения, интересы, надежность, поведение, местонахождение или передвижения».

относятся к правоохранительной деятельности и уголовному правосудию, может иметь важные последствия для объема применимых прав и обязательств[58]. В целом, исключения и отступления на основании правоохранительных оснований разрешены в Закон ЕС о защите данных в той мере, в какой они будут необходимыми и соразмерными, и если они будут сопровождаться гарантиями. В этом смысле статья 23 GDPR предусматривает, что как законы ЕС, так и национальные законы могут ограничивать объем определенных прав и обязательств, включая упомянутую статью 22 GDPR, если это необходимо для предотвращения, расследования, обнаружения или преследования уголовных преступлений или исполнения уголовных наказаний, включая защиту и предотвращение угроз общественной безопасности[59].

Статья 23 GDPR, описанная как «с самого начала весьма спорная», разрешает отклонения «от основного содержания GDPR», даже если «с такими же высокими требованиями» (Wagner & Benecke, 2016, 357).

В настоящее время нет официального обзора использования на уровне ЕС и на национальном уровне исключений и отступлений, основанных на этом положении[60]. Права, предоставленные субъектам данных в соответствии с LED, также могут быть ограничены посредством законодательных мер в порядке «чтобы не препятствовать официальным или юридическим расследованиям, расследования или процедуры во избежание нанесения ущерба предотвращению, расследованию, раскрытию или преследованию уголовных преступлений или исполнению уголовных наказаний»[61].

---

[58] Директива об электронной конфиденциальности в этом смысле предусматривает в своей статье 15 (1), что «государства-члены могут принимать законодательные меры для ограничения объема» определенных прав и обязательств, когда такие ограничения «представляют собой необходимую, уместную и соразмерную меру в пределах демократическое общество для защиты национальной безопасности (т.е. государственной безопасности), обороны, общественной безопасности, а также предотвращения, расследования, выявления и преследования уголовных преступлений».

[59] Статья 23 (1) (d) GDPR.

[60] Это известно, что в любом случае, большинство государств - членов воспользовались этим (см, например, раздел 41 Реализации Голландского Общих регулирований Закона о защите данных). Обычно возникают соображения правоохранительных органов: например, в Чешской Республике, когда на карту поставлены «защищенные интересы», такие как предотвращение, расследование или раскрытие уголовных преступлений, преследование уголовных преступлений, исполнение уголовных наказаний и защитные меры, соблюдение с обязательствами, связанными с осуществлением любого из прав субъекта данных из ст. 12–22 GDPR могут быть отложены (Zakonzedne 12. brezna2019 o zpracovanfosobnfch udaju (оригинал): Чешский закон № 110/2019 Coll., Закон от 12 марта 2019 г. об обработке персональных данных, раздел 6 (2) (b) и Раздел 11 (1)). Для этого просто необходимо уведомить DPA, уведомление, которое, тем не менее, не потребуется, если обработка, к которой это относится, осуществляется судами (там же, Раздел 11 (2)).

[61] Сольный концерт (44) LED. Чешский инструмент, заменяющий LED, чтобы продолжить аналогичный пример, предусматривает, что компетентные органы могут не выполнять запросы на осуществление права доступа, если это может поставить под угрозу выполнение задачи в области предотвращения, расследования и выявления преступных действий, правонарушения, преследование за уголовные правонарушения, исполнение уголовных наказаний и защитные меры (там же, раздел 28 (2)). В качестве меры предосторожности вводится обязательство вести учет причин, обосновывающих такое решение, в течение трех лет (Раздел 28 (4)).

Суд ЕС (CJEU) имеет значительную прецедентную практику в отношении законодательства ЕС о защите данных. Суд особо подчеркнул необходимость толкования его положений таким образом, чтобы гарантировать «эффективную и полную защиту» субъектов данных[62]. Особенно актуальным здесь является прецедентное право об обязательствах, налагаемых на поставщиков общедоступных телекоммуникационных услуг и сетей в отношении хранения данных, чтобы гарантировать, что данные, связанные с коммуникацией, доступны для целей расследования, обнаружения и судебного преследования серьезных преступлений, так же часто решения ИИ в области правоохранительной деятельности и уголовного правосудия основываются на использовании для таких целей данных, первоначально обработанных для других, иногда не связанных, целей, и вовлекают как частные компании, так и государственные органы.

Примечательным в этом контексте было решение CJEU по цифровым правам Ирландии[63], которое отменило Директиву 2006/24/ЕС[64] (известную как «Директива о хранении данных»), которая, основываясь на статье 15 (1) Директивы об электронной конфиденциальности, наложил ограничения на права и обязанности, установленные таким документом, в масштабах всего ЕС таким образом, который Суд описал как превышение «ограничений, налагаемых соблюдением принципа соразмерности в свете статей 7, 8 и 52 (1) Устава» (пункт 69). В частности, CJEU осудил, что Директива 2006/24/EC охватывает «в обобщенном виде всех лиц и все средства электронной связи, а также все данные трафика без каких-либо различий, ограничений или исключений, сделанных в свете цели: борьба с серьезными преступлениями» (параграф 57), и предупредил, что «тот факт, что данные сохраняются и впоследствии используются без уведомления подписчика или зарегистрированного пользователя, вероятно, вызовет в умах заинтересованных лиц ощущение, что их личная жизнь является предметом постоянное наблюдение» (пункт 37)[65].

---

[62] Cf. Google Испания Решение Суда (Большая Палата) от 13 мая 2014 г., Дело C-131/12, ECLI: EU: C: 2014: 317, пп. 34, 38, 53, 58.

[63] Digital Rights Ireland, Решение Суда (Большая палата) от 8 апреля 2014 г., объединенные дела C-293/12 и C-594/12, ECLI: EU: C: 2014: 238.

[64] Директива 2006/24/ЕС Европейского парламента и Совета от 15 марта 2006 г. о хранении данных, созданных или обработанных в связи с предоставлением общедоступных услуг электронной связи или сетей связи общего пользования, и изменяющая Директиву 2002/58 / EC, OJL 105,13.4.2006, стр. 54-63.

[65] В последующем решении по делу Tele2 Sverige и Watson CJEU постановил, что государства-члены не могут налагать на поставщиков услуг электронной связи обязательство общего и неизбирательного хранения данных, отмечая, что закон ЕС, читаемый «в свете статей 7, 8 и 11 и статью 52 (1) Хартии, следует толковать как исключающее национальное законодательство, которое в целях борьбы с преступностью предусматривает общее и неизбирательное хранение всего трафика и данных о местоположении всех подписчиков и зарегистрированных пользователей, относящихся к ко всем средствам электронной связи» (Решение Суда (Большая Палата) от 21 декабря 2016 г., Объединенные дела C-203/15 и C-698/15, ECLI: EU: C: 2016: 970, пункт 112). С тех пор CJEU регулярно сталкивается с дальнейшими делами, связанными с хранением данных, и, в частности, все еще должен выносить решения

Несмотря на важность для частных лиц, защита персональных данных, обрабатываемых для правоохранительных органов и уголовного правосудия, Европейская комиссия уделяла относительно ограниченное внимание, по крайней мере, по сравнению с GDPR как таковым. Работа Европейского совета по защите данных (EDPB) в этой области до сих пор также была заметно слабой, о чем свидетельствует отсутствие опубликованных руководств, рекомендаций или передовых методов на его официальном веб-сайте (см. Рисунок 1 ниже).

Figure 1: EDPB work on police and justice



Источник: Скриншот из https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recomendations-best-practices_en [по состоянию на 7 июля 2020 г.].

2.2.2. Правила обработки неличных данных

ИИ прямо упоминается в Регламенте (ЕС) 2018/1807 о свободном потоке неличных данных в ЕС[66], который направлен на обеспечение свободного потока неличных данных в пределах ЕС путем регулирования требований к

по соответствующим ссылкам на предварительное решение, направленное Государственным советом Франции (Объединенные дела C-511/18 и C-512/18), Courconstitutionnelle de Belgique (Дело C-520/18) и Трибунал по полномочиям расследований (Великобритания) (Дело C-623/17), в которых основной проблемой является применение Директивы об электронной конфиденциальности к деятельности, связанной с национальной безопасностью и борьбой с терроризмом - особенно в свете статьи 4 Договора о ЕС, согласно которой национальная безопасность является исключительной ответственностью каждого государства-члена. В феврале 2020 года Верховный суд Ирландии обсудил подачу запроса о предварительном решении по делу Двайер против комиссара Ан Гарда Сиочан (решение г-на судьи Кларка, главного судьи, вынесено 24 февраля 2020 года, Верховный суд, Грэм Дуайер против комиссара Гарда Сфочана, запись №: 2019/18), а также о хранении данных, гарантиях, связанных с доступом к данным, и действительности обвинительных приговоров, основанных на данных, полученных с помощью схем хранения данных (Hennessy, 2020).

[66] Регламент (ЕС) 2018/1807 Европейского парламента и Совета от 14 ноября 2018 г. о структуре свободного потока неличных данных в Европейском союзе, OJL303, 28.11.2018, стр. 59-68.

локализации данных, наличия такие данные компетентным органам, а также перенос данных для профессиональных пользователей. В изложении (9) этого Регламента действительно говорится, что ИИ, вместе с Интернетом вещей и машинным обучением, представляет собой основной источник неличных данных, которые могут принимать форму «агрегированных и анонимных наборов данных, используемых для анализа больших данных».

Положение о свободном потоке неличных данных не определяет «неличные данные», но использует этот термин как эквивалентный «электронным данным, отличным от персональных данных» (статья 2 (1)).

Он признает, что могут существовать наборы данных, в которых личные и неличные данные «неразрывно связаны», и в этом случае его положения не наносят ущерба применению GDPR (статья 2 (2)). Европейская комиссия опубликовала Руководство по взаимодействию между настоящим Регламентом и GDPR, в котором разъясняется, что понятие «неличные данные» в свободном потоке неличных данных должно определяться возражением (a contrario) против изложенных персональных данных на GDPR, и что могут быть как «неличные данные», которые изначально были таковыми, так и данные, которые сначала были личными, но стали «неличными» после анонимизации (COM (2019) 250 final, 4-5). В Руководстве признается, что «в большинстве реальных ситуаций набор данных, скорее всего, будет состоять как из личных, так и из неличных данных» (там же, 4).

Ключевой принцип Положения о свободном потоке неличных данных заключается в том, что такие неличные данные должны свободно передаваться в ЕС. Требования к локализации данных, относящиеся к государствам-членам, навязывающим обработку данных на своей территории или препятствующим обработке данных в другом государстве-члене, являются в принципе не допускается, если оправданы на основании общественной безопасности (не охватывающее необходимость содействия расследованию, выявление и преследование уголовных преступлений) в соответствии с принципом пропорциональности. Независимо от локализации данных, лица, на которых возложены обязательства по предоставлению данных компетентным органам, должны выполнять такие обязательства, обеспечивая и гарантируя эффективный и своевременный электронный доступ к данным компетентным органам[67]. Если указанные лица не будут выполнять требования, национальные компетентные органы должны оказывать друг другу помощь, при необходимости, в соответствии с инструментами в области сотрудничества полиции и уголовного правосудия, такими как Рамочное решение Совета 2006/960/JHA (известное как «Шведская инициатива»)[68], Директива 2014/41/ЕС

[67] Изложение (25) Положения о свободном распространении персональных данных.

[68] Рамочное решение Совета 2006/960/JHA от 18 декабря 2006 г. об упрощении обмена информацией и

о Европейский приказ о расследовании (EIO)[69] и Конвенция о киберпреступности[70].

В целом, Регламент представляет собой важный шаг в обеспечении доступа к неличным данным за пределами страны. Хотя он в исключительных случаях позволяет устанавливать требования к локализации данных на основе соображений безопасности, он, тем не менее, также предусматривает необходимость соблюдения определенных обязательств по предоставлению данных через границы и подтверждает актуальность механизмов, позволяющих осуществлять трансграничный доступ к данным, включая в правоохранительных целях.

3. Применение законодательства и уголовное правосудие

В этом разделе представлен обзор основных текущих тенденций, связанных с ИИ в области правоохранительной деятельности и уголовного правосудия, которые актуальны для обсуждения на уровне ЕС их воздействия на основные права. Они сгруппированы по четырем основным темам: «предсказуемая работа полиции», распознавание лиц, ИИ и уголовное правосудие, ИИ и границы.

Идея искусственного интеллекта, используемого для этих целей, намеренно широка. В соответствии с текущими разработками политики на уровне ЕС, охватываемое здесь понятие признает ключевыми компонентами разработок ИИ их зависимость от «данных», «алгоритмов» и «вычислительной мощности»[71]. Разложение ИИ на эти три основных элемента позволяет лучше понять преемственность и разрывы между ИИ и другими понятиями, которые ранее вызвали изменение политики и дискуссии в этой области, такие как «умное наблюдение», «профилирование» или «большие данные».

Термин «умное наблюдение» делает акцент на том факте, что новые решения должны быть «интеллектуальными» в том смысле, что они, кажется, «учатся» на наблюдаемых данных, а также «принимают решения» потенциально «самостоятельно» на основе определенных алгоритмов. В этом смысле было заявлено, что то, что лежит в основе дискуссий на уровне ЕС по

разведданными между правоохранительными органами государств-членов Европейского Союза, OJL 386, 29.12.2006, стр. 89-100.

[69] Директива 2014/41 / EU Европейского парламента и Совета от 3 апреля 2014 г. о Европейском порядке расследования уголовных дел, OJL 130, 1.5.2014, стр. 1-36.

[70] Конвенция Совета Европы о киберпреступности, CETS № 185.

[71] Cf. широкое видение ЕС, согласно которому «ИИ - это совокупность технологий, объединяющих данные, алгоритмы и вычислительную мощность» (COM (2020) 65 final, 2).

поводу ИИ, на самом деле является алгоритмически управляемой системой ADM [Automated Decision Making] (Penner, 2019).

Вообще говоря, слово «профилирование» связано с сортировкой людей на основе «компьютерного анализа больших наборов данных», который уже широко используется сотрудниками правоохранительных органов и пограничниками «для предотвращения, расследования и преследования уголовных преступлений, а также для предотвращения и выявления незаконной иммиграции» (FRA, 2018a, 7-8).

Термин «большие данные» обычно используется для обозначения обработки огромных наборов данных, включая наборы данных с данными разного происхождения. EDPS отметила, что в своей недавней Белой книге по ИИ Европейская комиссия опиралась на широкую концепцию ИИ, которую можно интерпретировать как охватывающую то, что другие называют «большими данными» (EDPS, Мнение 4/2020, 7). В прошлом «большие данные» ассоциировались с изменениями, которые могли иметь серьезные последствия – они изображались как уничтожение того, что считается криминальной информацией, того, что считается правильным аргументом, и даже того, как следует предотвращать, расследовать и преследовать преступление (Zavrsnik, 2017a, 3). В любом случае развитие систем искусственного интеллекта, в частности систем, основанных на машинном обучении, предполагает и способствует созданию огромных наборов данных, которые могут быть связаны с «большими данными» (Sartor & Lagioia, 2020, i), и сегодняшним искусственным интеллектом развитие во многом определяется данными (Boucher, 2019, 5).

Термин ИИ, возникающий в ходе этих дебатов, в целом и «плохо определен и потенциально вводит в заблуждение» (Babuta, Oswald & Rinik, 2018, 2). Кроме того, область ИИ является очень динамичной, поэтому самые тщательные усилия по определению ИИ и предоставлению рабочего определения и связанных таксономий и ключевых слов подчеркивают необходимость делать это всегда в контексте динамического процесса, подлежащего регулярным проверкам и итерациям. (Самойли и др., 2020, 6).

Размещение ИИ в контексте других, ранее существовавших политических дискуссий не направлено на отрицание его инновационного аспекта, но должно помочь понять, что дебаты вокруг ИИ не являются полностью уникальными и возникли не в пустом пространстве. Они появились среди многих других разработок, поощряющих использование компьютеров и алгоритмов и поддерживающих широкий доступ к данным, в том числе в том, что касается правоохранительных органов и уголовного правосудия.

Обработка данных в правоохранительных целях данных, которые изначально не собирались для таких целей, является проблемой, которая возникает регулярно, в том числе за рамками обсуждений ИИ[72]. Постоянное увеличение количества данных в наших обществах действительно сопровождалось на протяжении многих лет устойчивым интересом среди правоохранительных органов для доступа к любым возможным имеющимся данным. Такой интерес включает, например, интерес к данным, которыми владеют частные компании, включая данные, которые могут потребовать пересечения национальных границ (Carrera & Stefan, 2020, 3).

Наконец, разработки в этой области, связанные с искусственным интеллектом, также необходимо рассматривать на фоне прогрессивной «цифровой трансформации» государства. В этом смысле Специальный докладчик Организации Объединенных Наций (ООН) по вопросу о крайней нищете и правах человека описал в 2019 году появление «цифрового государства всеобщего благосостояния» во многих странах по всему миру, поскольку системы социальной защиты и помощи все больше основываются на технологиях «используется для автоматизации, прогнозирования, выявления, наблюдения, обнаружения, определения цели и наказания» (Специальный докладчик ООН по вопросам крайней бедности и прав человека, 2019, 1).

3.1 «Предиктивное наблюдение»

«Предсказательная полицейская деятельность» была описана как крылатая фраза, в основном на утверждении, что алгоритмическая обработка наборов данных позволяет выявить закономерности вероятных будущих правонарушений и виктимизации, которые, таким образом, могут быть пресечены до того, как они произойдут (Wilson, 2017, 108). Хотя истоки прогнозирующей полицейской деятельности можно проследить до экспериментов по компьютерному контролю над преступностью в 1970-х годах, и хотя прогнозирование в области преступлений и наказаний разрабатывалось и обсуждалось уже много десятилетий (Harcourt, 2008), этот термин в конечном итоге стал связан с ростом «больших данных» (Wilson, 2017, 109). Прогнозирование как обширная тенденция заметно повлияло на развитие безопасности во всем мире и, по крайней мере, в Европе з а последнее десятилетие, обычно связанное с предотвращением.

[72] EDPS, например, выразила озабоченность в июле 2020 года по поводу возможностей, предоставляемых Microsoft для возможного доступа к данным, связанным с использованием учреждениями ЕС ее продуктов и услуг третьим сторонам, включая правоохранительные или другие правительственные учреждения (EDPS, Outcome of ..., 24).

«Предсказательная полицейская деятельность» может принимать различные формы, и множество типологий были положены вперед. Методы прогнозирования полиции, например, можно разделить на четыре широкие категории: методы, направленные на прогнозирование преступлений или прогнозирование мест и времени с повышенным риском совершения преступлений; методы, направленные на прогнозирование правонарушителей или выявление лиц, которым грозит опасность совершения правонарушения (или повторного совершения преступления) в будущем; методы, направленные на прогнозирование личности преступников или создание профилей, аналогичных профилям прошлых преступников, и методы, направленные на прогнозирование жертв преступлений, используемые для выявления групп или лиц, которые могут стать жертвами преступлений (Perry et al., 2013, xiv). Типологии также могут быть основаны на возможных целях алгоритмического анализа данных или разведывательных данных в контексте полицейской деятельности: тогда можно выделить прогнозирующую полицейскую деятельность на макроуровне, включая стратегическое планирование, приоритизацию и прогнозирование; а также связывание и оценка оперативной информации, которая может включать, например, деятельность по снижению преступности; и принятие решений или оценка рисков в отношении отдельных лиц (Oswald & Grace, 2016, 3).

Электронный информационный центр конфиденциальности (EPIC) опубликовал в 2020 году отчет Министерства юстиции США бывшему президенту Обаме за 2014 год о прогнозной аналитике и алгоритмах в правоохранительных органах[73]. В отчете говорится, что использование «анализа социальных сетей» было «привлекает внимание некоторых государственных и местных правоохранительных органов» (Министерство юстиции США, 2014 г., стр. 3). К тому времени анализ социальных сетей начал использоваться для выявления людей, которые затем могут «получить повышенное внимание, дополнительные услуги поддержки или и то, и другое» (то же самое). Согласно отчету, большая часть анализа данных Федерального бюро расследований США (ФБР) нацелена на конкретные темы, хотя в некоторых случаях он использовался «для выявления подгрупп лиц, которые могут подлежать дальнейшему расследованию» (там же, 8). Информация, используемая для такого анализа данных, была описана как происходящая из «различных источников данных», включая коммерческие базы данных, и включающая, помимо прочего, биографические данные, биометрическую информацию, финансовую информацию, информацию о местонахождении, информацию о партнерах и аффилированных лицах, информацию о занятости и

[73] Отчет был получен после запроса, судебного иска и урегулирования путем переговоров в соответствии с Законом о свободе информации (FOIA): EPIC против Министерства юстиции, № 18-5307 (округ Колумбия).

бизнесе, визовую и иммиграционную информацию, информацию о поездке, и криминальную и следственную историю информации.

Инициативы «прогнозирующего полицейского надзора» возникли в разных государствах-членах, в основном с начала 2010-х гг., например, это были инициативы, так или иначе связанные с автоматическими системами контроля номерных знаков (Alfter, 2019, 52; Van Brakel, 2019, 44). Расширение использования алгоритмов полицией в последние годы было связано с тремя факторами: мерами жесткой экономии, которые ограничивают ресурсы и подталкивают к очевидно экономически более эффективным новым решениям; растущее понимание того, что полиция должна принять превентивную позицию, делая упор на предотвращение ущерба, а также увеличение объема и сложности имеющихся данных, что требует все более сложных инструментов обработки (Babuta & Oswald, 2020, vii).

Прогнозирование и предотвращение оказались особенно продуктивными в отношении отмывания денег и финансирования терроризма[74]. Текущие подходы в этой области действительно основаны на обязательствах, налагаемых на банки и другие обязанные субъекты, предпринимать соответствующие шаги для выявления и оценки рисков отмывания денег и финансирования терроризма с учетом факторов риска, в том числе связанных с их клиентами, странами или географическими регионами, продуктами, услугами, транзакциями или каналами доставки. Такая оценка риска организациями, действующими в качестве «привратников», в конечном итоге может привести к тому, что компетентные подразделения финансовой разведки (FIU) ЕС, которые имеют свои собственные обязательства по отчетности и обмену данными, могут сообщить о транзакциях, которые считаются подозрительными. Возможное обозначение определенных лиц как подозреваемых в ходе этого процесса может привести к ситуациям, требующим особого внимания, поднимая вопросы защиты данных, но также потенциально влияя на право на презумпцию невиновности (статья 48 Хартии основных прав ЕС)[75].

Прогностические подходы в правоохранительных органах часто основываются, на обработке данных, которые изначально не связаны с преступностью, а изначально собираются частными компаниями в контексте их

---

[74] См., В частности: Директива (ЕС) 2015/849 Европейского парламента и Совета от 20 мая 2015 г. о предотвращении использования финансовой системы в целях отмывания денег или финансирования терроризма, вносящая поправки в Регламент (ЕС) № 648/2012 Европейского парламента и Совета и отменяющую Директиву 2005/60 / ЕС Европейского парламента и Директиву Совета и Комиссии 2006/70/ЕС, OJL 141, 5.6.2015, с. 73-117. Также относится к отмыванию денег и финансированию терроризма: LIBE, 2020/2016 (INI), 5.

[75] Вопросы защиты данных стояли на переднем крае запрета, введенного EDPS 19 декабря 2019 года на операции обработки, выполняемые Европолом в рамках технической операции FIU.net, децентрализованной информационной сети, предназначенной для поддержки национальных подразделений финансовой разведки (EDPS, 2019, 41).

обычной деловой деятельности (например, банковское дело, телекоммуникации, путешествия). Схемы прогнозирующего полицейского контроля также обычно основываются на прогнозирующем программном обеспечении, выпускаемом частными компаниями, будь то поставщики, специализирующиеся в этой области (наиболее часто цитируемые, вероятно, компания PredPol) или крупные технологические корпорации (Wilson, 2017, 114).

В США в средствах массовой информации сообщается о практике частных компаний, нацеленных на рынок ИИ, которые будут активно включать сбор данных не особенно прозрачным образом для правоохранительных органов или с целью их последующего предоставления правоохранительным органам (Koebler, МИИberg & Cox, 2020). Например, в марте 2020 года появились обвинения в адрес компании Banjo, занимающейся искусственным интеллектом, в разработке приложений, специально предназначенных для тайного сбора данных из социальных сетей (Cox & Koebler, 2020).

Многие соответствующие события произошли в Соединенном Королевстве (Великобритания). Особенно интересны дискуссии вокруг Матрицы насилия в бандах (GVM), инструмента, используемого с 2012 г. Столичная полиция для выявления и оценки риска членов банд[76] по всему Лондону, причастных к насилию со стороны банд, а также для выявления тех, кто подвергается риску стать жертвой. GVM измеряет вред, который наносят люди, выставляя им баллы на основании доказательств совершения ими насилия и правонарушений, связанных с оружием, а также данных полиции о том, что у них есть доступ к оружию, или они участвуют в групповом насилии или подвергаются риску его совершения: отдельные лица, таким образом, классифицируются как красный, желтый или зеленый, что означает уровень риска (для потерпевших) или вреда (для правонарушителей), который они представляют[77]. База данных охватывает как взрослых, так и несовершеннолетних (MOPAC, 2018, 4).

По данным неправительственной организации Amnesty International, столичная полиция отказалась разглашать информацию о точных критериях, используемых для присвоения автоматических «оценок вреда» лицам, находящимся в матрице, и также будет неясно, как такие оценки могут быть связаны с какими-либо правоприменительными действиями (Amnesty International, 2018, 13-14).

---

[76] В этом контексте банда определяется как относительно устойчивая, преимущественно уличная группа молодых людей, которые считают себя (и воспринимаются другими) как заметную группу и участвуют в различных видах преступной деятельности и насилия.

[77] Об этом сообщает сайт столичной полиции.

В более общем плане НПО заявила, что практика обработки данных в базе данных и отсутствие надлежащих мер защиты создают риск того, что инструмент «дискриминирует и без того маргинализированных молодых людей с непропорционально сильным воздействием на чернокожих мальчиков и молодых мужчин» (там же, 3). Уведомление о принудительном исполнении было направлено в столичную полицейскую службу Управлением комиссара по информации (ICO) в 2018 году в связи с несоблюдением закона о защите данных. Считается, что с тех пор значительное количество людей было удалено из базы данных (Dodd, 2020).

Инициативы «прогнозирующего полицейского контроля» иногда могут полагаться на использование технологий распознавания лиц, которые, в свою очередь, редко развиваются отдельно от других разработок, более широко связанных с мониторингом общественных мест, например, для обнаружения «ненормального поведения» (например, Kayser-Bril, 2020).

3.2. Распознавание лиц

Технология распознавания лиц позволяет автоматически идентифицировать - или аутентифицировать - человека путем сопоставления черт лица на двух или более цифровых изображениях (EU FRA, 2019, 2). Согласно закону ЕС о защите данных, даже если обработка фотографий как таковая систематически не рассматривается как обработка, заслуживающая особой защиты, помимо общих правил защиты данных, когда данные обрабатываются для обеспечения такой идентификации или аутентификации, они должны рассматриваться как биометрические данные заслуживают особой защиты[78].

Использование технологий распознавания лиц не ограничивается областью правоохранительных органов и уголовного правосудия. Фактически, функция распознавания лиц вызвала большой интерес и споры во всем мире и в других областях, о чем свидетельствует коллективный иск в США против автоматизированной фотомаркировки Facebook и использования ею программного обеспечения для сопоставления лиц, чтобы предлагать имена людей в фото пользователей[79].

С глобальной точки зрения использование распознавания лиц некоторыми конкретными государствами было особенно противоречивым; В этом смысле следует упомянуть международную озабоченность по поводу использования распознавания лиц в Китае для идентификации членов

[78] См., В частности, подробное описание (51) и ст. 4 (14 и 9 (1)) GDPR; статьи 3 (13) и 10 LED.
[79] Иск урегулирован в январе 2020 г.: Singer & Isaac, 2020 г.

уйгурского меньшинства, в основном мусульманской группы (Mozur, 2019). Распознавание лица в общественных местах, как говорят, особенно быстро растет в России (Light, 2019).

В правоохранительной области использование распознавания лиц, которое привлекло больше внимания, касается распознавания лиц в реальном времени.

В 2016 году в американском отчете предупредили о широком использовании распознавания лиц в реальном времени в стране, предупредив, что уже в то время несколько крупных полицейских управлений активно изучали распознавание лиц в реальном времени на видео с камеры наблюдения в реальном времени (Garvie, Bedoya & Frankle, 2016)[80]. Документируя различные проблемы, связанные с этими событиями, включая вопросы конфиденциальности и предвзятости, а также угрозы свободе слова, авторы настоятельно призвали принять законодательство, регулирующее использование правоохранительными органами поиск по распознаванию лиц, особенно для большей прозрачности, с предупреждением, что «распознавание лиц слишком мощно, чтобы быть секретным» (там же).

Некоторые города США, такие как Сан-Франциско и Бостон, запретили определенные виды использования распознавания лиц на своей территории (Vaas, 2020). В Детройте продолжается судебный процесс между Американским союзом гражданских свобод (ACLU) и Департаментом полиции Детройта, связанный с делом человека, который был неправомерно арестован на основании ошибочной идентификации с помощью программного обеспечения для распознавания лиц (Lee, 2020). По-прежнему в США участники кампании противодействуют распространению распознавания лиц в университетских городках, в частности, на основании того, что они описали как системные расовые и гендерные предубеждения в развернутых системах (Fight for the Future, 2020).

В июне 2020 года Комитет по технологической политике США (USTPC) Ассоциации вычислительной техники (ACM) призвал немедленно приостановить частное и государственное использование технологий распознавания лиц «при всех известных или разумно предсказуемых обстоятельствах, которые могут нанести ущерб установленным человеческим и правовым нормам права», в ожидании принятия соответствующего всеобъемлющего закона и нормативных актов, регулирующих его использование, надзора за его применением и смягчения потенциального вреда (ACM USTPC, 2020, 1). Призыв был основан на оценке, что технология

[80] Первоначальное развертывание «интеллектуальной системы видеонаблюдения» на общественных улицах в США восходит к 2001 году; первое использование считается, что из этих технологий используются в тюрьмах (Gates, 2011, 54 и 64).

слишком часто дает результаты, демонстрирующие явную предвзятость, основанную на этнических, расовых, гендерных и других человеческих характеристиках, характеристиках, которые ACM USTPC, тем не менее, описал как «распознаваемые компьютерными системами» (то же самое).

Политические дискуссии по поводу распознавания лиц широко распространены в Великобритании, где ряд полицейских сил полагается на эти системы. В Лондоне, например, столичная полиция использует функцию распознавания лиц в режиме реального времени, чтобы «помочь в борьбе с серьезным насилием, преступлениями с применением огнестрельного оружия и ножей, сексуальной эксплуатацией детей и помочь защитить уязвимых»[81]. Великобритания, в частности, финансирует исследовательский проект по стимулированию неограниченной возможности биометрии лица, представленный как потенциально значительный вклад в повестку дня правительства Великобритании в области безопасности в рамках умных городов и национальной безопасности[82]. Столичная полицейская служба является одним из участников проекта вместе с китайским академическим учреждением, и Министерство внутренних дел Великобритании один из партнеров проекта[83].

В 2019 году Высокий суд Англии и Уэльса заявил, что использование технологии автоматического распознавания лиц для сопоставления лиц людей с полицейскими списками наблюдения было законным в деле, касающемся программы, пилотируемой уже несколько лет в Южном Уэльсе. Полиция, называемая AFR Locate[84]. Программа описывается полицией Южного Уэльса как развертывание технологии автоматического распознавания лиц в режиме реального времени, которая сравнивает изображения лиц в режиме реального времени с предварительно определенным списком наблюдения, чтобы «определить местонахождение» интересующих людей, генерируя возможные совпадения, которые рассматриваются оператором (-ами)[85]. В оценке использования технологии распознавания лиц полицией Южного Уэльса в 2018 году было отмечено, что правовые инструменты, связанные с ней, и этические принципы, которые они излагают, предшествуют типам «Возможности, предоставляемые технологиями APR», добавляя, что «такая новая нормативно-

---

[81] См. Онлайн-информацию MET о распознавании лиц в реальном времени.

[82] Project Face Matching for Automatic Identity Retrieval, Recognition, Verification and Management, FACER2VM, EP / N007743 / 1, январь 2016 г. - сентябрь 2021 г.

[83] То же. См. Также: См. Также: Privacy International, 2020d.

[84] R (по заявлению Эдварда Бриджеса) против главного констебля Южного Уэльса [2019] EWHC 2341.

[85] См. Специальный веб-сайт полиции Южного Уэльса: http://afr.south-wales.police.uk/. «Лица, представляющие интересы» определяются как люди, разыскиваемые по ордерам и подозреваемые в определенных преступлениях,
но также как потенциально пропавшие без вести и уязвимые люди, а также люди, разыскиваемые в разведывательных целях.

правовая база, вероятно, будет необходима по мере того, как эта технология получит более широкое распространение» (Davies, Innes & Dawson, 2018, 41).

На протяжении многих лет организации гражданского общества на международном уровне озвучивали ряд призывов к приостановке использования определенных видов использования технологии распознавания лиц. Декларация Public Voice 2019 года Мораторий на технологию распознавания лиц для массового наблюдения не только призывает к такой приостановке, но также призывает страны «установить правовые нормы, технические стандарты и этические принципы, необходимые для защиты основных прав и соблюдения юридических обязательств перед дальнейшем развертыванием этой технологии»[86].

Особо спорный вопрос касается роли частных компаний в развертывании этих технологий. В феврале 2020 года СМИ сообщили, что согласно просочившимся документам компания Clearview ИИ имела контракты с тысячами правоохранительных органов, компаний и частных лиц по всему миру, а также в Европе (Mac, Haskin & McDonald, 2020). Сервисы Clearview ИИ, которые он формально нацелен на «активных сотрудников правоохранительных органов»[87], можно охарактеризовать как состоящие в сопоставлении людей с онлайн-изображениями, снятыми с различных платформ (Hill, 2020). Например, служба позволяет, следователю загрузить фотографию человека, «представляющего интерес», и выполнить поиск в базе данных, составленной Clearview ИИ, того, что представлено как «общедоступные изображения», размещенные кем-то в Интернете (Blatt, 2020) - не обязательно человек, о котором идет речь. Некоторые из платформ, с которых Clearview ИИ, по-видимому, захватил изображения, официально возражали против такой очистки изображений Clearview ИИ (Porter 2020).

В марте 2020 года Шведское управление по защите данных (DatИИnspektionen) сообщило, что оно расследует возможное использование услуг Clearview ИИ государственными органами Швеции (DatИИnspektionen, 2020). В июле 2020 года ICO и Австралийский комиссар по информации объявили, что начали совместное расследование в отношении Clearview ИИ, сосредоточив внимание на использовании им «очищенные» данных и биометрических данных людей (ICO, 2020).

В письме в ответ на озабоченность, высказанную рядом депутатов Европарламента относительно возможного использования продуктов Clearview ИИ правоохранительными органами ЕС, датированное 10 июня 2020 года, EDPB отметило, что такие органы могут при определенных обстоятельствах

[86] Полный текст и список подписавших лиц доступны здесь: https://thepublicvoice.org/ban-facial-recognition/.
[87] См. https://dearviewai.tvpeform.com/to/SFnULY.

использовать технологии распознавания лиц для проверки изображений против шаблонов «в базах данных, которые находятся под контролем официальных органов и которые были созданы в соответствии с законодательством Союза или государства-члена», но что «возможное использование услуги, такой как предлагаемая Clearview ИИ, правоохранительными органами, однако, будет быть принципиально другим, так как это будет означать, в рамках полицейского или уголовного расследования, обмен личными данными с частной стороной за пределами Союза и биометрическое сопоставление таких данных с массовой и произвольно заполненной базой данных фотографий и фотографий лиц, доступных в Интернете» (Jelinek, 2020). EDPB добавила, что «сомневается в том, что какой-либо закон Союза или государства-члена обеспечивает правовую основу для использования такой услуги, как предлагаемая Clearview ИИ», отметив, что «несколько членов EDPB уже начали дополнительные запросы об использовании таких средств для лица, технологий признания в их соответствующих юрисдикциях», и выразил готовность внести свой вклад в дальнейшие дискуссии по этим вопросам (то же самое).

Clearview ИИ - не единственная компания, о которой публиковались отчеты о договоренностях с правоохранительными органами. Принадлежащая Amazon компания Ring, компания по производству устройств интеллектуальной безопасности, в основном известная продажей интерактивных видеодомофонов, как сообщается, заключила ряд соглашений с правоохранительными органами, в том числе в Европе (Privacy International, 2020b), которые могут касаться или не относиться конкретно к распознавание лиц или другие технологии, связанные с ИИ.

Использование технологий распознавания лиц в общественных местах вызвало споры во многих странах мира. Так обстоит дело, например, в Бразилии, где установка в общественном метро системы для показа рекламы, основанной на автоматическом «определении» эмоций, пола и возраста прохожих, привела к судебному разбирательству со стороны Бразильского института защиты прав потребителей (IDEC) (Arroyo & Leufer, 2020).

В ЕС внедрение распознавания лиц в общественных местах, в том числе в тестовом режиме, как правило, вызывает самые разные реакции. В 2017 году общественность была разделена, когда на железнодорожных станциях Берлина было запущено полевое испытание программы распознавания лиц (Furstenau, 2017).

Также была реакция со стороны судебных органов и DPA. В Бельгии DPA остановило развертывание камер распознавания лиц в аэропорту Завентем, не имевшее законного основания (Peeters, 2020). Во Франции административный суд объявил недействительным в феврале 2020 года решение регионального совета, позволяющее протестировать систему наблюдения, основанную на

распознавании лиц, для контроля доступа к двум средним школам[88]. В решении критиковалось отсутствие предварительной оценки воздействия и основа обработки персональных данных на согласии заинтересованного лица или его родителей, несмотря на то, что их отношения с учреждениями сделали невозможным предоставление действительно свободного согласия. Это решение последовало за жалобой, поданной вместе с другими ассоциациями неправительственной организацией La Quadrature du Net, также активно оспаривающей использование распознавания лиц для наблюдения за участниками демонстраций (La Quadrature du Net, 2019).

В августе 2019 года Шведский DPA оштрафовал муниципалитет на 200000 человек за использование технологии распознавания лиц для контроля посещаемости учащихся школ (EDPB, 2019). Распознавание лиц применялось в контексте пилотного проекта на основе согласия отдельных лиц, но DPA посчитало, что согласие не является действительной правовой основой в таком контексте, учитывая явный дисбаланс между субъектом данных и контролером (то же самое). Однако то же DPA разрешило правоохранительными органами определенные виды использования распознавания лиц (Barik, 2019).

До сих пор технологии распознавания лиц применялись в общественных или полуобщественных местах как государственными органами, так и частными компаниями. В Испании, например, недавно в некоторых супермаркетах были развернуты системы распознавания лиц, предположительно для того, чтобы автоматически обнаруживать лиц, на которых может распространяться запретительный судебный приказ, не позволяющий им входить в помещения или приближаться к работникам супермаркета (Rubio, 2020). DPA ЕС иногда разрешает определенные виды использования функции распознавания лиц в реальном времени частными лицами - например, DPA Дании разрешает использование этой функции футбольным клубом у входа на свой стадион для идентификации лиц, которым запрещено посещать футбольные матчи (IT-Pol, 2019) .

В 2020 году некоторые крупные компании, такие как IBM, объявили, что в будущем воздержатся от определенной коммерческой деятельности, связанной с распознаванием лиц (Peters, 2020).

[88] Tribunal administratif de Marseille (9eme chambre), № 1901249, 27 февраля 2020 г.

3.3. ИИ и следствие

Разработки, связанные с искусственным интеллектом, основанные на все более широком использовании данных, вычислений и алгоритмов, также пронизывают администрирование правосудия[89], включая уголовное правосудие. Истоки некоторых текущих событий можно проследить до появления «компьютеризированного правосудия» как тенденции, направленной на повышение подотчетности и предсказуемости судебных решений путем сокращения полномочий судей, которые некоторые при некоторых обстоятельствах считают чрезмерными. (Франко Аас, 2005, 65).

ИИ используется или исследуется в европейских правовых системах для различных целей, таких как облегчение доступа к закону (например, через чат-ботов), поддержка альтернативных мер урегулирования споров по гражданским делам, разрешение споров в режиме онлайн или «профилирование судей»[90]. способы, которыми практика, связанная с ИИ, попала в суды, связаны с расчетом рисков неправомерного поведения, например, для алгоритмического испытательного срока (Wilson, 2017b, 144). Тем не менее, использование инструментов прогнозирования судьями в уголовных процессах в Европе, иногда называемых «алгоритмическим правосудием» или «автоматизированным правосудием», по крайней мере, до недавнего времени описывалось как очень редкое (Ronsin & Lampos, 2018, 37).

Алгоритмы рецидивов привлекли большое внимание, особенно в США. Многие из опасений, поднятых по поводу использования алгоритмов для целей уголовного правосудия, относятся к косвенным расовым предубеждениям в моделях, которые предсказывают правонарушение и повторное правонарушение, например, путем использования косвенных переменных, которые не являются нейтральными. Исследование ProPublica, проведенное в 2016 году в системе профилирования исправительных правонарушителей для альтернативных санкций (COMPAS), показало, что чернокожие обвиняемые почти в два раза чаще подвергаются риску совершения правонарушения, чем белые обвиняемые (Babuta, Oswald & Rinik, 2018, 7, отмечая, однако разработчик системы оспорил анализ; Заврсник, 2017б, 145).

Вопросы, связанные с гарантиями надлежащей правовой процедуры, также вышли на первый план, наиболее известный из них - дело State v.

---

[89] Justice охватила цифровые технологии несколькими способами, такими как разрешение споров в Интернете, где алгоритмы играют все более важную роль (Katsh & Rabinovich-Einy, 2017).

[90] Cf. Приложение II, сопровождающее Европейскую этическую хартию по использованию искусственного интеллекта в судебных системах и их окружении, принятую CEPEJ на 31-м пленарном заседании (Страсбург, 3-4 декабря 2018 г.), CEPEJ (2018) 14.

Loomis[91], постановление Верховного суда штата Висконсин постановило, что использование судом первой инстанции алгоритмической оценки риска при вынесении приговора не нарушает права ответчика на надлежащую правовую процедуру (даже несмотря на то, что методология, используемая для проведения оценки, о которой идет речь, не была раскрыта), тем не менее, была введена процессуальная гарантия, чтобы предупредить судей об ограничениях таких оценок. Еще одно интересное дело в США касалось судебного разбирательства в Вашингтоне, округ Колумбия, в котором оспаривалось использование инструмента оценки рисков Структурированной оценки насилия и риска среди молодежи (SAVRY) в процессе вынесения приговора несовершеннолетним: с помощью этого инструмента было установлено, что молодой человек, которому обещали испытательный срок в обмен на признание вины, тем не менее, был «высоким риском» и должен был быть заключен в тюрьму (Richardson, Schultz, Southerland, 2019, 9). Адвокаты оспорили оценку SAVRY, оспаривая ее научную надежность, и выиграли спор, убедив судью запретить использование инструмента в конкретном случае, о котором идет речь (там же, 10)[92].

Великобритания представляет собой хороший пример разработок в этой области с помощью алгоритмического «инструмента оценки риска вреда» (HART), разработанного в 2017 г. полицейскими силами Дарема для оценки риска повторного совершения правонарушений отдельными лицами в целях поддержки принятия решений об опеке (Бабута, Освальд & Риник, 2018, 6). Инструмент генерирует оценку риска, которая становится одним из ряда факторов, которые сотрудники-кадры должны учитывать при проведении общей оценки риска (то же самое). Этот инструмент вызвал разногласия, в частности, из-за того, что изначально он полагался на использование данных сегментации потребителей от частной компании, позже отложенных в сторону (Grace, 2019, 6).

Вообще говоря, использование судебных систем искусственного интеллекта критически зависит от доступности данных, что привело к признанию подхода открытых данных к судебным решениям в качестве предварительного условия для работы юридических технологических компаний, специализирующихся на поисковых системах или анализе тенденций (так называемый «предсказуемое правосудие») (Ronsin & Lampos,

---

[91] 881 N.W2d 749 (Висконсин, 2016 г.).

[92] Другие соответствующие дела включают дело «Луизиана против Хикерсона», касающееся использования правоохранительными органами города Нового Орлеана базы данных оценки рисков под названием Gotham, созданной компанией Palantir (Ричардсон, Шульц, Саутерленд, 2019 г., стр. 13); База данных в принципе была развернута для выявления лиц, которые могут стать преступниками или жертвами огнестрельного насилия, которым должны были быть отправлены информационные сообщения об их образе жизни, но, похоже, они сыграли роль в расследованиях, приведших к предварительному судебному разбирательству против г-на Хикерсон (там же, 14).

2018, 16). Однако обработка таких данных вызывает ряд проблем, которые касаются закона о защите данных, но также и других, которые касаются возможности изменения в формировании судебной практики (то же самое).

Исследователи отметили, что, хотя этот тип инструментов в настоящее время используется для ограниченных целей, у технологии есть потенциал, чтобы сделать гораздо больше, и отсутствие нормативно-правовой базы для ее использования вызывает обеспокоенность. (Бабута, Освальд и Риник, 2018, стр.7).

3.4. ИИ и границы

Есть множество случаев, когда алгоритмы уже актуальны в пограничном контексте. Автоматизированные системы принятия решений становятся все более и более распространенными по отношению к границам во всем мире и могут включать системы, которые классифицируют людей (например, как группы высокого риска или высокого приоритета); которые генерируют баллы, оценки вероятности и другие показатели, поддерживающие принятие решений человеком; что «помечает» дела для рассмотрения или расследования; которые предоставляют рекомендации по приложениям или даже принимают полные решения (Molnar & Gill, 2018, 3).

3.4.1. Общие тенденции

В ЕС связанные с границами крупномасштабные информационные системы, включающие алгоритмическую обработку, обычно связаны посредством различных потоков данных с правоохранительными органами - национальными властями, Европолом или часто с обоими. Данные, исходящие от правоохранительных органов, могут поступать в системы, связанные с границами, и данные из этих систем могут в конечном итоге предоставляться или предоставляться правоохранительным органам. Безопасность и управление границами уже много лет являются основными движущими силами роста централизованных и децентрализованных информационных систем в AFSJ[93].

Интерес государственных органов к данным, которые будут обрабатываться в целях миграции и убежища, похоже, растет во многих государствах-членах. Некоторые из них, например, в последние годы внесли правовые изменения в свои национальные процедуры предоставления

[93] Обзор см., Например: COM (2016) 205 final.

убежища, в частности, чтобы дать властям возможность собирать и анализировать данные с личных устройств (например, смартфонов) от лиц, ищущих убежища[94], также увеличивая обязанности заявителей сотрудничать (EMN, 2019, 6). Данные могут быть проанализированы, чтобы помочь установить их личность и маршруты путешествий (там же, 21). Государства – члены также усиливают пограничный контроль, вкладывая средства в техническое оборудование для пограничных проверок (например, «электронные ворота», биометрические проверки личности, киоски и т. д.), Включая средства распознавания лиц (там же, 54). Технологии, используемые на границах, разнообразны и могут включать автоматизированные системы наблюдения с различными возможностями обнаружения (например, обнаружение сердцебиения и тепловизионные камеры) (то же самое).

Во всем мире на протяжении многих лет наблюдается тенденция к увеличению обязательств по раскрытию данных для лиц, пересекающих границу. В США продолжающийся судебный процесс оспаривает обязательство, наложенное с 2019 года на заявителей на визу, раскрывать учетные записи в социальных сетях (EFF, 2020).

На уровне ЕС заметным событием стало введение в 2019 году EDPS временного запрета на публикацию отчетов о мониторинге социальных сетей Европейским офисом поддержки убежища (EASO). EASO использовало такие отчеты для предоставления руководству и соответствующим заинтересованным сторонам информации «об изменениях в маршрутах предоставления убежища и миграции и предложениях о контрабанде, а также для обзора разговоров в сообществе социальных сетей по ключевым вопросам, таким как бегство, торговля людьми и другие системы и процессы предоставления убежища» (EDPS, 2019, 30). EDPS осудила, что это произошло без необходимых юридических оснований и соответствующие меры предосторожности и подчеркнул, что «официальные инструменты мониторинга СМИ в целом вызывают ряд серьезных проблем с защитой данных», которые в этом случае «включали сдерживающий эффект - тенденцию пользователей самоцензурировать свой онлайн-контент, если они считают, что за ним можно наблюдать - высокие риски, связанные с основными правами лиц и групп, за которыми ведется наблюдение, отсутствие справедливости и прозрачности участвовали в обработке этих данных, и огромное количество пользователей социальных сетей, причастных к этому»[95].

---

[94] В Германии продолжается судебный процесс, в котором ставится под сомнение законность мер, действующих с 2017 года, позволяющих государственным органам получать доступ к данным, хранящимся в мобильных устройствах просителей убежища, с целью предотвращения мошенничества с убежищем (Reuters, 2020).

[95] EDPS, Годовой отчет 2019, Люксембург: Бюро публикаций Европейского Союза, 2019, стр. 30.

В AFSJ ЕС крупномасштабные информационные системы все чаще включают алгоритмическое принятие решений. Как правило, в соответствующих законодательных документах это представлено в различных терминах, отличных от ИИ, включая, например, ссылки на «метод анализа данных» (COM (2018) 302 final, 9). Независимо от терминологии, как правило, на карту поставлено то, что помимо выявления «известных» конкретных подозреваемых, некоторые инструменты содержат функцию алгоритмического профилирования, которая идентифицирует «неизвестных» лиц, которые могут представлять интерес для правоохранительных органов и органов управления границами (EU FRA, 2018a, 114).

В 2016 году Европейский парламент обратился к Европейской комиссии с просьбой запустить пилотный проект по обзору основных прав инструментов и программ ЕС по сбору данных. В конечном итоге проект выразил озабоченность по поводу воздействия на основные права «функций профилирования», включенных как в существующие, так и в будущие информационные системы ЕС (FGB, 2019, 4).

Большое количество разработок в этой области объединяется в eu-LISA, Агентстве ЕС, обеспечивающем оперативное управление крупномасштабными системами информационных технологий (IT) ЕС и их соответствующей коммуникационной инфраструктурой, в AFSJ: Eurodac (Европейская база данных оцифрованные отпечатки пальцев лиц, ищущих убежища, и нелегальных мигрантов), Шенгенскую информационную систему (SIS) (облегчающую обмен информацией о лицах и объектах между национальной полицией, пограничным контролем, таможенными, визовыми и судебными органами) и Визовой информационной системой (VIS), который поддерживает реализацию общей визовой политики ЕС, позволяя специализированным национальным властям вводить и просматривать данные, в том числе биометрические данные, для краткосрочных виз в Шенгенскую зону. Eu-LISA в настоящее время разрабатывает другие будущие общеевропейские информационные системы: систему въезда / выезда (EES), Европейскую систему информации и разрешений на поездки (ETIAS) и Европейскую систему информации о судимости для граждан третьих стран (ECRIS-TCN), а также их компоненты функциональной совместимости и играет решающую роль в технической реализации и развитии функциональной совместимости информационных систем ЕС, как это предусмотрено пакетом совместимости 2019 года[96].

[96] Cf. Регламент (ЕС) 2019/817, устанавливающий основу для взаимодействия между информационными системами ЕС (границы и визы), и Регламент (ЕС) 2019/818, устанавливающий основу для взаимодействия между информационными системами ЕС (сотрудничество полиции и судебных органов, убежище и миграция), OJ Л 135, 22.5.2019, стр. 27-84; и Регламент (ЕС) 2019/818 Европейского парламента и Совета от 20 мая 2019 г. о создании основы для взаимодействия между информационными системами ЕС в области полицейского и

Более подробное изучение ETIAS может помочь понять некоторые из проблем основных прав, связанных с этими разработками, которые являются относительно парадигматическими и, таким образом, полезны для определения места EES и предстоящего «обновления» VIS[97]. До этого обсуждались вопросы, связанные с алгоритмической обработкой данных, относящихся к путешествию.

3.4.2. PNR

Профилирование путешественников – не новость в ЕС. Состоялись серьезные юридические и политические дискуссии в отношении обработки данных записей регистрации пассажиров (PNR), будь то передача таких данных в третьи страны или в контексте системы PNR ЕС. Первоначально, что было особенно сложным был вопрос о том, как кадр, с точки зрения права ЕС, использование в правоохранительных целях данных, первоначально собранных частными компаниями для коммерческих целей[98]. В конце концов, вопросы сосредоточены на основных требованиях с точкой зрения фундаментального права на обработку данных по схемам PNR.

Европейский парламент запросил в CJEU Заключение о соглашении о передаче данных PNR в Канаду, которое было согласовано с властями Канады, в частности, в отношении совместимости предполагаемого соглашения с обязательствами, вытекающими из Хартии ЕС. В заключении, вынесенном в июле 2017 года, подчеркивается ряд серьезных сбоев[99]. Отмечая, что предусмотренное соглашение разрешает «систематическую и непрерывную передачу данных PNR всех авиапассажиров, выполняющих рейсы между Европейским союзом и Канадой»[100], которые могут использоваться в качестве «инструмент разведки»[101] Суда отметил, что данные PNR были «предназначен для анализа систематически до прибытия воздушного судна в Канаде автоматизированных средств, на основе заранее установленные моделей и критериев», а также автоматически уточнена cross-checking с другими базами

судебного сотрудничества, предоставления убежища и миграции и внесения поправок в Регламент (ЕС) 2018/1726, (ЕС) 2018/1862 и (ЕС) 2019/816, OJL 135, 22.5.2019, стр. 85-135.

[97] В 2018 году Европейская комиссия опубликовала предложение о постановлении Европейского парламента и Совета по обновлению Визовой информационной системы (VIS) (COM (2018) 302 final). Модернизация, представленная

в предложении, в частности, основана на введении использования «индикаторов риска», содержащих «правила анализа данных, а также конкретные значения, предоставленные государствами-членами, и статистику, полученную из других соответствующих баз данных по управлению границами и безопасности» (ibid., 9).

[98] Cf. Решение Суда (Большой палаты) CJEU от 30 мая 2006 г., Европейский парламент против Совета Европейского Союза (C-317/04) и Комиссии Европейских сообществ (C-318/04), ECLI: EU: C: 2006: 346.

[99] CJEU, Заключение 1/15 от 26 июля 2017 г. («EU Canada PNR»), ECLI: EU: C: 2017: 592.

[100] Там же, п. 127.

[101] Там же, п. 131.

данных[102], и что этот анализ может «привести к дополнительным проверкам на границах в отношении авиапассажиров, которые, как было установлено, могут представлять риск для общественной безопасности, и, при необходимости, на основе этих проверок, к принятию индивидуальных решений, имеющих обязательную силу воздействия на них»[103]. Он отметил, что эти анализы должны были проводиться «без объяснения причин, основанных на индивидуальных обстоятельствах, которые позволили бы сделать вывод о том, что соответствующие лица могут представлять риск для общественной безопасности»[104].

CJ EU заявил, что «степень вмешательства, которое влечет за собой автоматический анализ данных PNR в отношении прав, закрепленных в статьях 7 и 8 Хартии, по существу зависит от заранее установленных моделей и критериев, а также от баз данных, на которых этот тип обработки данных основывается»[105], и, как следствие, «заранее установленные модели и критерии должны быть конкретными и надежными[106], что позволяет достигать результатов, ориентированных на лиц, которые могут находиться под «разумным подозрением» в причастности к террористическим преступлениям или серьезным транснациональным преступлениям и не должно носить дискриминационный характер»[107].

Система PNR ЕС была создана Директивой (ЕС) 2016/681 («Директива PNR ЕС») в 2016[108]. Она применяется, как общее правило, к данным «рейсов за пределы ЕС», хотя государства-члены также могут ее расширить на «рейсы внутри ЕС». Созданная им система в некотором роде напоминает описанный выше общий подход к предотвращению отмывания денег в той степени, в которой обязательства по обработке данных возлагаются на авиаперевозчиков, которые должны поддерживать связь со специальными национальными отделами информации о пассажирах (PIUs). Однако в этом сценарии процедуры

---

[102] То же.
[103] Там же, п. 132.
[104] То же.
[105] Там же, п. 172.
[106] В связи с этим, а также «поскольку автоматизированный анализ данных PNR обязательно предполагает некоторую погрешность», любой положительный результат, полученный в результате автоматизированной обработки этих данных, должен (...) подлежать индивидуальной повторной проверке не «Автоматизированные средства до принятия индивидуальной меры, отрицательно влияющей на соответствующих авиапассажиров» (пункт 173).
[107] То же. В отношении этого последнего пункта CJEU провозгласил, что «для обеспечения того, чтобы на практике предварительно установленные модели и критерии, их использование и используемые базы данных не носили дискриминационного характера и ограничивались тем, что строго необходимо, надежность и актуальность этих заранее установленных моделей, критериев и используемых баз данных должна, с учетом статистических данных и результатов международных исследований, быть охвачена совместным обзором выполнения предусмотренного соглашения» (пункт 174).
[108] Директива (ЕС) 2016/681 Европейского парламента и Совета от 27 апреля 2016 г. об использовании данных регистрации пассажиров (PNR) для предотвращения, обнаружения, расследования и преследования террористических преступлений и серьезных преступлений, OJL119, 4.5.2016, стр. 132-149.

оценки риска не должны выполняться частными компаниями, которые несут ответственность только за предоставление собранных данных. PIUs несут ответственность за сбор, хранение и дальнейшую обработку таких данных PNR, за передачу их компетентным органам и за обмен ими с PIUs других государств-членов, а также с Европолом.

Одним из наиболее обсуждаемых вопросов по реализации Директивы ЕС PNR было участие Европола в разработке и распространении «общих наборов индикаторов, правил таргетинга и профилей рисков» (Президентство в Совете, 6300/19, 2019). В 2019 году большинство (88%) государств-членов заявили, что было бы «отличной идеей», если бы Европол мог внести свой вклад в разработку правил и показателей таргетинга, «из-за его центрального положения и его важной роли в сборе и обмене информацией по правилам таргетинга и / или профилям риска» и действовать как «депозитарий» общих правил и индикаторов (там же, 14). Некоторые государства-члены, однако, отметили, что каждая ОРП и государство-член должны решать, будут ли они предлагать Европолу разработать такие наборы и в какой степени эти наборы будут считаться обязательными. Состоялись также дискуссии о том, действительно ли идея о том, что Европол может предложить централизованное хранилище всех показателей и правил таргетинга, используемых на национальном уровне, что, по-видимому, приемлемо для некоторых, является хорошей идеей, и некоторые государства – члены рассматривали это как потенциальное нарушение информационной безопасности, которое может поставить под угрозу их (national PIUs) эффективность (там же 9).

CJEU, как ожидается, править по совместимости Директивы ЕС PNR и ЕС основных прав. Незавершенное дело (дело C-817/19) действительно касается запроса о предварительном решении Конституционного суда Бельгии, поданного в октябре 2019 года после действий ассоциации Ligue des droits humИИns по транспонированию Директивы ЕС о PNR в Бельгии. Вопросы, переданные в Суд, относятся, в частности, к систематической предварительной оценке данных всех пассажиров (Конституционный суд Бельгии, 2019 г.), то есть «предварительной оценке», производимой путем сравнения данных о пассажирах с базами данных и заранее определенными критериями, которые применяются «в систематическим и обобщенным образом, независимо от того, есть ли какие-либо объективные основания полагать, что соответствующие пассажиры могут представлять опасность для общественной безопасности[109]. В январе 2020 года Окружной суд Кельна также направил в CJEU запрос о вынесении предварительного решения, в контексте разбирательства, возбужденного Gesellschaft Fur Freiheitsrechte (GFF) и рядом истцов (TurB, 2020). Одним из истцов, ведущих судебный процесс в Германии, является

[109] См. Заявление в CJEU по делу C-817/19.

бывший глава секретариата Комитета по гражданским свободам, правосудию и внутренним делам Европейского парламента (Комитет LIBE) (De Capitani, 2019).

3.4.3. ETIAS

Европейская система информации и разрешений на поездки (ETIAS) касается разрешений на поездки для граждан третьих стран, освобожденных от визовых требований для въезда в Шенгенскую зону, на основании «рассмотрения того, что присутствие этих граждан третьих стран на территории государств ЕС будет представлять угрозу безопасности, нелегальной иммиграции или высокого риска эпидемии»[110]. Уполномоченные органы государств – членов и Европол могут обращаться к данным, хранящимся в центральной системе ETIAS, с целью предотвращения, обнаружения и расследования террористических преступлений или других серьезных уголовных преступлений[111]. При использовании ETIAS соответствующие соображения при принятии решения о разрешении на поездку возникают до прибытия путешественников на внешние пункты пересечения границы. Его использование должно быть факультативным только в течение первых шести месяцев с даты начала работы[112], но обязательно после этого. Следует отметить, что разрешение на поездку не дает автоматического права въезда или пребывания[113].

На практике кандидаты должны подать заявку онлайн или через приложение[114], предоставляя запрошенные личные данные[115]. Затем представленные данные сравниваются с данными, уже имеющимися в центральной системе ETIAS, а также с данными в SIS, EES, VIS, Данные Евродак, Европола и Интерпола[116], и список наблюдения ETIAS[117]. Некоторые

---

[110] См. Ст. 1 (1) Регламента (ЕС) 2018/1240 Европейского парламента и Совета от 12 сентября 2018 г., устанавливающего Европейскую систему информации о поездках и разрешений (ETIAS) и вносящих поправки в Регламент (ЕС) № 1077/2011, (ЕС) № 515/2014, (ЕС) 2016/399, (ЕС) 2016/1624 и (ЕС) 2017/226, 20JL 236,19.9.2018, стр. 1-71 (далее «Регламент ETIAS»).

[111] Арт. 1 (2) Регламента ETIAS.

[112] Арт. 83 (1) Регламента ETIAS.

[113] Арт. 36 (6) Регламента ETIAS.

[114] Арт. 15 (1) Регламента ETIAS.

[115] Арт. 17 (2) Регламента ETIAS.

[116] Данные Интерпола - это данные из базы данных Интерпола по проездным документам, связанным с уведомлениями (TDAWN) и из базы данных Интерпола по украденным и утерянным проездным документам (SLTD). В ответ на вопрос об опасениях по поводу использования в политических целях «красных уведомлений»
в этих базах данных Европейская комиссия пояснила в 2019 году, что связь из этих баз данных должны быть выдержаны в Интерпол предоставление необходимых гарантий (ответ г. Аврамопулос от имени Европейской Комиссии Вопрос: E-000204/2019, 5 апреля 2019 года).

[117] Список наблюдения ETIAS «должен состоять из данных, касающихся лиц, подозреваемых в совершении

личные данные также сравниваются с рядом показателей риска: это относится, в частности, к дате и месту рождения, полу, национальности, имени (именам) родители заявителя, домашний адрес, образование и род занятий[118].

Если есть совпадение, то есть совпадение, эта информация записывается в файл приложения[119]. Если совпадение произошло из-за совпадения данных, исходящих от SIS, например, потому что кандидат был зарегистрирован как заслуживающий «осторожных проверок или чеков», ссылка на это будет добавлена в файл заявки[120]. В конечном итоге, в случае попадания, национальное подразделение ETIAS государства-члена, идентифицированного как ответственное, должно выдать или отказать в разрешении на поездку[121]. Когда попадание связано с совпадением с индикатором риска, «национальное подразделение ETIAS ответственного государства-члена должно оценить безопасность, нелегальную иммиграцию или высокий эпидемический риск и решить, выдать ли разрешение на поездку или отказать в нем», и «ни при каких обстоятельствах национальное подразделение ETIAS ответственного государства-члена не может принимать решение автоматически на основе попадания на основании конкретных показателей риска», поскольку этот риск должен оцениваться «индивидуально»[122].

Статья 33 Регламента ETIAS объясняет, что то, что система предусматривает, представляет собой тип «профилирования», как это определено в GDPR: данные, предоставленные заявителями, должны сравниваться с «конкретным риском индикаторы, установленные центральным подразделением ETIAS» и «указывающие на безопасность, нелегальную иммиграцию или высокие эпидемические риски». Алгоритм, обеспечивающий такое профилирование, называется «правилами проверки ETIAS».

Именно Европейская комиссия определит посредством делегированного акта, что следует рассматривать как «риски, связанные с безопасностью,

---

террористического преступления или другого серьезного уголовного преступления или участия в них, или лиц, в отношении которых имеются фактические указания или разумные основания, основанные на общей оценке лица, для полагают, что они совершат террористическое преступление или другое серьезное уголовное преступление» (ст. 34 (1) Регламента ETIAS). Европол или государство-член, добавляющее данные в список наблюдения ETIAS, должны оценить, «является ли информация адекватной, точной и достаточно важной для включения» (Статья 35 (1) (a)).
Они также должны «оценить потенциальное влияние данных на долю заявок, обрабатываемых вручную», оценка предположительно сложная и в любом случае должна быть автоматизирована, как eu-LISA, «должна создать специальный инструмент» для таких целей оценка (ст. 35 (2)), технические характеристики которой определяются Европейской комиссией посредством имплементационных актов (ст. 35 (7)).

[118] Арт. 20 (5) Регламента ETIAS.

[119] Ст. 20 (7) Регламента ETIAS. В случае совпадения центральная система ETIAS обращается к центральному блоку ETIAS, который обращается к файлу и дважды проверяет его действительность (статья 22 Регламента ETIAS).

[120] Статья 23 Регламента ETIAS.

[121] Статья 26 (2) Регламента ETIAS.

[122] Статья 26 (6) Регламента ETIAS.

нелегальной иммиграцией или высоким эпидемическим риском»[123]. Должно быть принято во внимание для этих целей, в частности, статистика EEE по аномальные показатели передержки и отказы записи «для а конкретной группы путешественников», статистика ETIAS об аномальных темпах отказов разрешений на поездки в связи с безопасностью, нелегальной иммиграцией или высоким эпидемическим риском «связанным с конкретной группой путешественников»: статистика по корреляция между данными и задержкой путешественников или отказами во въезде; предоставленная государствами-членами «информация, подтвержденная фактическими и доказательными элементами», о конкретных индикаторах риска или угрозах безопасности или о ненормальных показателях задержек и отказов во въезде для «определенной группы путешественников», а также предоставленная информация о конкретных высоких эпидемических рисках государств-членов, а также данные эпидемиологического надзора и оценки риска, предоставленные Европейским центром профилактики и контроля заболеваний (ECDC), а также информацию о вспышках заболеваний, о которых сообщает ВОЗ.

На основе описанных рисков будут определены «индикаторы рисков», которые затем позволят центральному подразделению ETIAS установить «конкретные индикаторы риска, состоящие из комбинации данных, включающих одну или несколько из этих категорий данных: (а) возрастной диапазон, пол, национальность; (б) страна и город проживания; (в) уровень образования (начальное, среднее, высшее или нулевое); (г) текущая профессия (рабочая группа). В Положении отмечается, что эти «конкретные индикаторы риска должны быть целевыми и соразмерными». Он также запрещает использование индикаторов риска, «основанных исключительно на поле или возрасте человека», что оставляет некоторую двусмысленность в отношении того, будут ли допустимыми факторами риска на основании сочетания пола и возраста (например, «женщины старше ...» или «мужчины моложе ...»). Индикаторы риска «ни при каких обстоятельствах не должны основываться на информации, раскрывающей цвет лица, расу, этническое или социальное происхождение, генетические особенности, язык, политические или иные взгляды, религию или философские убеждения, членство в профсоюзе, принадлежность к национальному меньшинству, собственность, рождение, инвалидность или сексуальная ориентация»[124]. Тем не менее, как уже отмечалось, они могут быть основаны, например, на уровне образования или группе работы. Таким образом, двери, ведущие к возможной неправомерной дискриминации, закрыты не полностью[125].

---

[123] Статья 33 (2) Регламента ETIAS.
[124] Статья 33 (5) Регламента ETIAS.
[125] Cf. также в этом смысле: ФГБ, 2019, 33.

Информационная система ETIAS, которая включает центральную систему ETIAS со списком наблюдения ETIAS, будет находиться под управлением eu-LISA[126]. Центральное подразделение ETIAS будет находиться в руках Frontex, Европейского агентства пограничной и береговой охраны[127]. Это центральный блок. Подразделение в Frontex, которому поручено «определение, создание, предварительную оценку, внедрение, оценку постфактум, пересмотр и удаление конкретных индикаторов риска», используемых для составления профиля путешественников, после консультации со скрининговым советом ETIAS[128]. Это тот же центральный отдел, который будет нести ответственность за «проведение регулярных аудитов» реализации индикаторов риска, «в том числе путем регулярной оценки их воздействия на основные права, в частности, в отношении конфиденциальности и защиты персональных данных»[129]. Комиссия по отбору ETIAS, которая должна выполнять консультативную функцию, работать в рамках Frontex и состоять из представителей различных национальных подразделений ETIAS, самого Frontex и Европола[130]. Консультативный совет может, если сочтет «это уместно, обратитесь к ETIAS Fundamental Совет по руководству по правам[131] по конкретным вопросам, связанным с основными правами, в частности, в отношении конфиденциальности, защиты личных данных и недискриминации»[132].

Что касается основных прав, поставленных на карту, Регламент ETIAS уделяет особое внимание праву на недискриминацию. Статья 14, озаглавленная «Недискриминация и основные права», тем не менее, помимо общего запрета на любую обработку персональных данных, может «привести к дискриминации в отношении граждан третьих стран по признаку пола, расы, цвета кожи, этнического или социального происхождения, генетические особенности, язык, религия или убеждения, политические или иные взгляды, принадлежность к национальному меньшинству, собственность, рождение, инвалидность, возраст или сексуальная ориентация», необходимость полного уважения «человеческого достоинства и неприкосновенности, а также основных прав, включая право на уважение частной жизни и защиту личных данных». В нем

---

[126] Ст. 6 Регламента ETIAS.
[127] Ст. 7 Регламента ETIAS.
[128] Ст. 7 (2)(c) Регламента ETIAS. По словам ОЛР ЕС, система ETIAS будет опираться на алгоритм, разработанный Fronted (EU FRA, 2018a, 114).
[129] Ст. 7 (2)(e) Регламента ETIAS.
[130] Ст. 9 (1) Регламента ETIAS.
[131] Руководящий совет ETIAS по основным правам, на который возложена как консультативная, так и «оценочная» функция, должен состоять из сотрудника по основным правам в Frontex и представителей консультативного форума по основным правам Frontex, EDPS, EDPB и EC. FRA. Совет по руководству по основным правам ETIAS должен проводить регулярные оценки и давать рекомендации Совету по отбору ETIAS относительно воздействия на основные права обработки заявок и профилирования в рамках ETIAS, «в частности, в отношении конфиденциальности, защиты персональных данных и недискриминации», иметь доступ к упомянутым аудитам и публиковать годовой отчет (статья 9 (5) Регламента ETIAS).
[132] Арт. 9 (5) Регламента ETIAS.

также упоминается, что «особое внимание следует уделять детям, пожилым людям и лицам с ограниченными возможностями», и что «наилучшие интересы ребенка должны быть в первую очередь рассмотрены». Следует подчеркнуть, что это положение как таковое не препятствует определению индикаторов рисков, основанных на том факте, что определенные «группы путешественников» были связаны с определенными более высокими связанными рисками, будь то риски для безопасности, предполагаемая склонность к «просрочке», или риски для здоровья.

В происхождении ETIAS и ЭЭС можно проследить до публикации пакета Смарт границ Европейской комиссией в 2013 году. Этот пакет последовал запуском пилотного проекта Смарт границ, который включал в себя этап тестирования доказательства концепции с эксплуатационные испытания в различных пунктах пропуска. Результаты проекта, представленные eu-LISA, перекликаются с мелкомасштабным опросом, проведенным FRA, который показал, что большинство путешественников из третьих стран выразили озабоченность по поводу надежности системы, особенно в отношении возможных сбои в работе и трудности, связанные с исправлением любых неточных данных (eu-LISA, 2015a, 12). Результаты исследования FRA показали, что «наиболее вероятные последствия неверных данных в системе въезда и выезда касаются рисков лиц, ошибочно отмеченных как чрезмерно задержанные, и использования такой информации со стороны полиции, иммиграционной службы или других должностных лиц», что потенциально может привести к «риску быть задержанным» (eu-LISA, 2015b, 307). FRA также отметило, что «автоматизированные системы могут быть запрограммированы для идентификации людей с использованием конфиденциальных данных, таких как раса, этническая принадлежность или состояние здоровья», и заявило, что «меры, чтобы избежать дискриминационного профилирования, следовательно, необходимы» (то же самое).

EDPS предупредил, что система ETIAS «может представлять риск для основных прав и свобод ЕС» и что «эффективное применение мер защиты данных в рамках ETIAS является особенно сложной задачей», поскольку предлагаемые запланированные операции по обработке данных включают обмен данными между контроллерами, которые подпадают под различные правила защиты данных ЕС (EDPS, 2019, 22). Он также предупредил, что существует риск того, что «людям будет очень трудно эффективно осуществлять свои права на защиту данных» (то же самое).

Действительно, в этой системе применяемые правила защиты данных особенно сложны[133]. В соответствии с Регламентом ETIAS центральный блок

[133] Арт. 56 Регламента ETIAS. В контексте ETIAS Регламент EU-DP применяется к обработке персональных данных компаниями Frontex и eu-LISA; GDPR применяется к обработке персональных данных национальными

ETIAS должен предоставлять широкой общественности всю необходимую информацию в отношении подачи заявки на разрешение на поездку[134], которое должно включать ссылки на права субъектов данных в соответствии с Регламентом EU-DP, GDPR, Регламентом Европола и LED[135]. Неясно, была ли такая общая информация или будет ли эффективно разъяснять, к каким операциям обработки применимы, какие именно права и как соответствующие права будут реализованы.

Регламент ETIAS гласит, что когда люди предоставляют данные в систему, они должны быть проинформированы о существующих процедурах, применимых к осуществлению их прав в соответствии со статьями 13–16 Регламента (ЕС) 2001/45 (теперь замененного EU-DPR), и статьи 15–18 GDPR. Важно отметить, что эта индивидуальная информация, следовательно, не включает в себя никакой информации о правах на возражение против профилирования (статья 21) и правах, связанных с автоматическим принятием решений (статья 22) GDPR. Также не упоминаются эквивалентные права в EU-DPR[136]. На самом деле, Регламент ETIAS только прямо указывает на возможное осуществление прав доступа, исправления, завершения, удаления личных данных и ограничение обработки, а не дополнительные права[137].

4. Влияние на основные права

Многие участники уже приложили много усилий для выявления влияния систем искусственного интеллекта на основные права в целом. В Белой книге Европейской комиссии по ИИ отмечается, что ИИ «может причинить вред», и далее отмечается, что вред может быть несущественным, например, включая «потерю конфиденциальности, ограничение права на свободу выражения мнения, человеческое достоинство, дискриминацию в доступе к занятости» (COM (2020) 65 final, 10). В почти столь же странной формулировке он также

подразделениями ETIAS в отношении оценки заявок пограничными и иммиграционными властями, но не в тех случаях, когда обработка выполняется в национальных подразделениях ETIAS компетентными органами, оценивающими заявки для целей предотвращение, обнаружение или расследование террористических преступлений или других серьезных уголовных правонарушений, и в этом случае должен применяться LED, хотя, когда национальное подразделение ETIAS фактически принимает решение о разрешении на поездку как таковое, всегда применяется GDPR. Кроме того, LED должен применяться, когда компетентные национальные органы получают доступ к центральной системе ETIAS для целей предотвращения, обнаружения и расследования террористических преступлений или других серьезных уголовных преступлений, подпадающих под их компетенцию, а также Регламента Европола, когда именно Европол получает доступ к данным для аналогичных целей.

[134] Арт. 71 Регламента ETIAS.

[135] Арт. 71 (q) Регламента ETIAS.

[136] Право на возражение и права, связанные с автоматизированными индивидуальными решениями, были в ст. 18 и 19 Регламента (ЕС) 2001/45.

[137] Арт. 64 Регламента ETIAS.

выдвигает, что «основные риски, связанные с использованием ИИ, касаются применения правил, направленных на защиту основных прав (включая личные данные, защиту конфиденциальности и недискриминацию), а также безопасность» (там же, 10). В Белой книге в конечном итоге более прямо признается, что «использование ИИ может повлиять на ценности, на которых основан ЕС, и привести к нарушениям основных прав», будь то в результате недостатков в общей конструкции систем ИИ или в результате использования данных без исправления возможной систематической ошибки (там же, 11).

В предыдущем разделе уже приводился ряд примеров, в которых разработки, связанные с системами искусственного интеллекта в области правоохранительной деятельности и правосудия, рассматривались как оказывающие влияние на основные права. В этом разделе более подробно рассматриваются некоторые из наиболее часто поднимаемых вопросов. Он не пытается связать конкретные типы воздействия с конкретными событиями или областями, поскольку проблемы - а также сами затронутые права - обычно взаимосвязаны: например, было указано, что недостатки в системах прогнозирующей полицейской деятельности могут «создавать длительные последствия, которые распространятся на всю систему уголовного правосудия и общество в более широком смысле» (Richardson, Schultz & Crawford, 226). Было заявлено, что отсутствие правил автоматического профилирования ставит под угрозу само понятие свободы (Graf, 2017, 451).

В 2019 году Комитет экспертов по вопросам прав человека при автоматизированной обработке данных и различных формах ИИ (MSI-AUT) при Совете Европы утверждал, что алгоритмические системы принятия решений, основанные на методах профилирования на основе данных, могут угрожать нескольким людям права, включая право на справедливое судебное разбирательство и надлежащую правовую процедуру, право на свободу выражения мнений и информации, право на защиту от дискриминации при осуществлении прав и свобод, а также право на неприкосновенность частной жизни и защиту данных (MSI-AUT, 2019, 8).

Рекомендация Совета Европы о влиянии алгоритмических систем на права человека от апреля 2020 года утверждает, что существуют «серьезные проблемы для прав человека, связанные с растущей опорой на алгоритмические системы в повседневной жизни, например, в отношении права на справедливое судебное разбирательство; право на конфиденциальность и защиту данных; право на свободу мысли, совести и религии; право на свободу выражения мнения; право на свободу собраний; право на равное обращение; экономические и социальные права»[138].

[138] Рекомендация CM / Rec (2020) 1, Приложение, пункт A.4.

Существует общее мнение о том, что системы искусственного интеллекта могут быть развернуты в области правоохранительной деятельности и уголовного правосудия, что делает возможное влияние на основные права еще более значительным[139]. Наконец, важно отметить, что акцент на основных правах в этой сфере исследование не должно позволять игнорировать тот факт, что использование ИИ в этой области может также вызвать другие типы вопросов об их влиянии[140].

4.1 Конфиденциальность и защита данных

Хотя права на уважение частной жизни и защиту личных данных признаны отдельно в Хартии основных прав ЕС (в статьях 7 и 8 соответственно), в соответствии с ЕКПЧ гарантии защиты данных составляют аспект статьи 8 о праве уважать частную жизнь.

Прецедентное право Европейского суда по правам человека (ЕСПЧ) по статье 8 ЕКПЧ и надзору обширно[141]. Суд особо подчеркнул, что возможность получения правительствами подробного профиля наиболее интимных аспектов жизни граждан путем сопоставления различных типов данные «могут привести к особо инвазивному вмешательству в частную жизнь», с явной ссылкой в этом контексте «на взгляды, выраженные Судом Европейского Союза и Европейским парламентом».[142] В этом смысле крайне важно иметь в виду, что технологии, связанные с ИИ, такие как распознавание лиц, упрощают связывание личных данных между различными системами наблюдения и объединение профилей (Datenethikkommission, 2019, 102).

Ключевым вопросом для ЕСПЧ является требование предсказуемости любых мер наблюдения. Дело в Свободе[143] касалось перехвата сообщений и

---

[139] В этом смысле учет воздействия ИИ при использовании в уголовном судопроизводстве, например, был описан как «даже более важный» из-за их прямого воздействия на личные свободы людей (Ronsin & Lampos, 2018, 39).

[140] Например, о влиянии прогнозируемой работы полиции на подотчетность полиции: Hardyns & Rummens, 2017, 214.

[141] В отношении борьбы с терроризмом ЕСПЧ особо подчеркнул, что «это противоречило бы цели усилий правительства по сдерживанию терроризма, тем самым восстанавливая веру граждан в свои способности поддерживать общественную безопасность, если бы террористическая угроза была парадоксальной заменяется предполагаемой угрозой беспрепятственного вторжения исполнительной власти в частную жизнь граждан со стороны благодаря неконтролируемым, но далеко идущим методам наблюдения и прерогативам» (Сабо и Висси против Венгрии, постановление от 12 января 2016 г., п. 68).

[142] Szabo and Vissy, параграф 70, в отношении цифровых прав / пересмотра / решения CJEU и Резолюции Европарламента по программе наблюдения АНБ США, касающийся, в частности, «все более размытых границ между правоохранительной и разведывательной деятельностью, приводящих к с каждым гражданином обращаются
как с подозреваемым и за ним наблюдают, как это было воспринято после «разоблачений Сноудена» 2013 года (EP, 2014,7)

[143] Свобода и другие против Соединенного Королевства, решение от 1 июля 2008 г.

последующего использования «фильтрации» методы, состоящие из автоматической системы сортировки, работающей под контролем человека и направленной на выбор сообщений на основе того, что иногда называлось «списками ключевых слов», «техническими базами данных» или «Словарем»[144]. Суд пришел к выводу, что применимое право на тот момент не указывало «с достаточной ясностью, чтобы обеспечить адекватную защиту от злоупотребления властью, объем или способ осуществления очень широкой свободы усмотрения, предоставленной государству для перехвата и изучения внешних сообщений»[145]. В частности, в законе не было «изложено в общедоступной форме какое-либо указание на процедуру отбора для изучения, обмена, хранения и уничтожения перехваченных материалов», и, таким образом, вмешательство в права заявителей в соответствии со статьей 8 ЕКПЧ не могут рассматриваться как «соответствующие закону»[146].

Среди необходимых гарантий, регулярно выдвигаемых ЕСПЧ на первый план, выделяется уведомление лиц, за которыми ведется наблюдение. Уведомление не обязательно должно происходить во время меры наблюдения, но может происходить и после этого, то есть, как только это не поставит под угрозу цель меры наблюдения. Такое «последующее уведомление о мерах наблюдения неразрывно связано с эффективностью средств правовой защиты в судах и, следовательно, с существованием эффективных гарантий против злоупотребления полномочиями по наблюдению», - заявил Суд[147].

Недавнее судебное решение по делу Гограна от 13 февраля 2020 г.[148], касалось сохранения профиля ДНК, отпечатков пальцев и фотографии осужденного[149]. В ходе судебного разбирательства обсуждался вопрос о том, можно ли получить доступ к базе данных, хранящей фотографии, для целей распознавания лиц, что, очевидно, было невозможно изначально (параграф 13), но в конечном итоге стало возможным (параграфы 37, 68), поскольку данные могли быть переданы в другую базу данных, которая имел функции распознавания лиц (параграф 69). В постановлении ЕСПЧ прямо отклонил аргумент, представленный правительством Великобритании, согласно которому «чем больше данных сохраняется, тем больше преступлений предотвращается», отметив, что «принятие такого аргумента в контексте схемы

---

[144] Там же, пункт 43.
[145] Там же, пункт 69.
[146] То же.
[147] Вебер и Саравия против Германии, 29 июня 2006 г., пункт 135.
[148] Гогран против Соединенного Королевства, жалоба № 45245/15, ECLI: CE: ECHR: 2020: 0213JUD004524515, [2020] ECHR 144.
[149] Конкретно, неизбирательный характер полномочий хранить такие данные, без ссылки на серьезность правонарушения или необходимость бессрочного хранения и в отсутствие какой-либо реальной возможности пересмотра. ЕСПЧ пришел к выводу, что такое удержание не могло считаться соразмерным рассматриваемым обстоятельствам, которые включали отсутствие каких-либо соответствующих гарантий и отсутствие какого-либо реального пересмотра, и, таким образом, составляло нарушение статьи 8 ЕКПЧ.

бессрочного хранения будет означать такая практика равносильна оправданию хранения информации обо всем населении и их умерших родственниках, что определенно будет чрезмерным и неуместным» (параграф 89).

Еще одно очень интересное решение было вынесено ранее в этом году в Нидерландах в отношении оценки рисков государственными органами. В феврале 2020 года Окружной суд Гааги вынес действительно знаменательное решение[150] о системе индикации системного риска (SyRI) - инструменте, который правительство Нидерландов создало для борьбы с мошенничеством. Дело было инициировано несколькими группами гражданского общества, включая голландскую секцию Международной комиссии юристов и двух частных лиц. Голландский законодатель определил SyRI как техническую инфраструктуру со связанными процедурами, с помощью которых данные могут быть связаны и проанализированы с целью создания отчетов о рисках. Наличие отчета о рисках означало бы, что лицо было признано достойным расследования в отношении возможного мошенничества, совершения злоупотреблений или несоблюдения законодательства[151].

В своем решении Окружной суд отметил, что «новые технологии – включая цифровые возможности для связывания файлов и анализа данных с помощью алгоритмов – предлагают (больше) возможностей для правительства обмениваться данными между его органами власти в контексте их законодательных норм обязанность предотвращать мошенничество и бороться с ним» и заявил, что «следует использовать эти новые технологические возможности для предотвращения и борьбы с мошенничеством» (параграф 6.4). Однако Суд также отметил, что «развитие новых технологий также означает, что право на защиту личных данных приобретает все большее значение» (параграф 6.5). Поскольку эти технологии могут серьезно влиять на жизнь людей, но самим людям сложно оценить такой эффект, законодатель несет «особую ответственность» при применении таких инструментов, как SyRi (параграф 6.85).

Анализ Суда привел к выводу, что законодательство по SyRi не отвечало установленным требованиям в статье 8 (2) ЕКПЧ, которая разрешает вмешательство в право на уважение частной жизни только, которое может

---

[150] Решение Окружного суда Гааги от 5 февраля 2020 г., номер дела C/09/550982, ECLI: NL: RBDHA: 2020: 865 . Приговор был отмечен тем, что остановил инициативу, основанную на искусственном интеллекте, по «обнаружению мошенничества до того, как оно произойдет», и поставил под наблюдение с этой целью заявителей о социальном обеспечении, включая людей в наиболее уязвимых ситуациях (Privacy International, 2020c).

[151] Инструмент может использоваться по запросу определенных государственных органов или других органов с публичной функцией, таких как муниципальные власти, Налоговая и таможенная администрация Нидерландов, Инспекция по социальным вопросам и занятости или Служба иммиграции и натурализации. Персональные данные, обработанные SyRI, включали данные о работе, образовании, налогах, собственности, жилье, административных мерах и санкциях, гражданской интеграции, основаниях для исключения из льгот, пенсии, долговом бремени, реинтеграции, социальных льготах и некоторые данные медицинского страхования.

считаться необходимым в демократическом обществе, что означает, что оно должно быть необходимым, соразмерным и вспомогательным по отношению к намеченной цели. В этом контексте Суд отметил, что, рассмотрев действующую систему в свете основных принципов обработки данных, установленных Хартией ЕС и GDPR, в частности, принципов прозрачности, ограничения целей и минимизации данных, система была «недостаточно прозрачной и поддающейся проверке» (пункт 6.7).

В отношении этих пробелов он отметил, что действующее законодательство не предоставляет четкой информации о фактических данных, которая могла бы обоснованно привести к выводу о наличии повышенного риска (параграф 6.87) в отношении функционирования модели риска, в отношении методы анализа рисков, валидация модели риска и проверка индикаторов риска (параграф 6.89). Было неясно, как субъекты данных «могли защитить себя от того факта, что о них был представлен отчет о рисках», и в целом знать, были ли данные о них обработаны на правильных основаниях, что противоречит принципу, что «данные субъект должен иметь разумную возможность отслеживать свои личные данные» (параграф 6.90).

В отношении проблем, создаваемых искусственным интеллектом для закона о конфиденциальности и защите данных, в Белой книге Европейской комиссии по ИИ утверждается, что GDPR и Директива об электронной конфиденциальности «устраняют эти риски», но допускают, что «может возникнуть необходимость проверить, могут ли системы искусственного интеллекта создают дополнительные риски» (COM (2020) 65 final, 11)[152]. Это намекает на тот факт, что люди «все больше будут подвергаться действиям и решениям, принимаемым системами ИИ или с их помощью, которые иногда могут быть трудными для понимания и эффективно бороться там, где это необходимо», но также и то, что «ИИ увеличивает возможности для отслеживания и анализа повседневных привычек людей», в том числе «государственными органами или другими организациями для массового наблюдения» (то же самое). Более того, «ИИ может также использоваться для отслеживания и деанонимизации данных о людях, создавая новые риски для защиты персональных данных даже в отношении наборов данных, которые сами по себе не включают персональные данные», - заявляет ЕС.

[152] В частности, в отношении GDPR, ЕС заявляет, что он будет «постоянно отслеживать и оценивать его применение» (COM (2020) 65 final, 11).

4.3 Свобода слова и информации, а также свобода собраний и ассоциаций

Некоторые вмешательства в права на неприкосновенность частной жизни и защиту данных могут одновременно иметь прямое негативное влияние на права на свободу выражения мнений и информации (статья 11 Хартии ЕС) и / или право на свободу собраний и ассоциаций (статья 12 Хартии ЕС), что на самом деле также может быть затронуто, даже если на карту не будут поставлены статьи 7, 8 Хартии ЕС. Значительные проблемы возникают при развертывании технологий искусственного интеллекта для мониторинга общественных мест – например, с помощью распознавания лиц в реальном времени и мониторинга коммуникаций, например, в социальных сетях. Групповая анонимность может подвергаться особому давлению (EU FRA, 2019, 29).

В Белой книге Европейской комиссии по ИИ отмечается, что обработка персональных данных, связанная с ИИ, может вызвать новые риски для основных прав, которые влияют на права, отличные от защиты личных данных и конфиденциальности, такие как право на свободу выражения мнений и политические свободы, в частности когда ИИ используется онлайн-посредниками для определения приоритетов информации и модерации контента (COM (2020) 65 final, 11).

Это связано с растущей в последние годы озабоченностью по поводу использования автоматизированных процессов модерации онлайн-контента, которые могут серьезно повлиять на право на свободу выражения мнений, но также и на право на недискриминацию[153]. Эти опасения еще более усугубляются общей проблемой отсутствия прозрачности в отношении коммуникационных процессов и применения интернет-службами инициатив по борьбе с дезинформацией (Van Hoboken et al., 2019, 124). Важно подчеркнуть, что в отношении дезинформации в Интернете часто сосуществуют призывы к поддержке инструментов ИИ для мониторинга достоверности информации и призывы усилить прозрачность используемых алгоритмов, особенно в отношении пользователей (Группа высокого уровня по поддельным новостям и дезинформации в Интернете, 2018).

[153] См., Например: Комитет экспертов по качественной журналистике в эпоху цифровых технологий (MSI-JOQ), 2019, 15.

4.4 Недискриминация

Риски предвзятости и дискриминации, вызванные алгоритмическим принятием решений, очень часто подчеркиваются. Агентство ЕС по основным правам отметило, что «прямая или косвенная дискриминация посредством использования алгоритмов, использующих большие данные, все чаще рассматривается как одна из самых насущных проблем использования новых технологий» (EU FRA, 2018b, 3). Рекомендация Совета Европы о правах человека влияние алгоритмических систем на права человека в апреле 2020 года отмечает, что «любые алгоритмические системы используют методы оптимизации», которые основаны на установлении приоритета определенных ценностей над другими, что «может вызвать неблагоприятные последствия, особенно для меньшинств и маргинализированных или обездоленных групп»[154].

В отношении «прогнозирующей полицейской деятельности» важный вопрос касается самой актуальности возможного включения алгоритмических переменных, таких как криминальное прошлое и семейное прошлое, которые могут заставить прошлое поведение определенной группы решить судьбу человека, который, тем не менее, «уникальный человек с особым социальным происхождением, образованием, навыками, степенью вины и отличительными мотивами для совершения преступления» (Ronsin & Lampos, 2018, 39). Это связано с опасностью создания «эхо-камер, в которых могут быть закреплены уже существующие предрассудки» (MSI-NET, 2018, 11), и в которых люди могут оказаться в ловушке без их ведома[155].

Кроме того, исследователи показали, как некоторые используемые системы, особенно в США, построены на данных, полученных в периоды некорректных, расово предвзятых и даже незаконных практик и политик («грязная полиция»), которые неизбежно повлияли на сам процесс

---

[154] Рекомендация CM / Rec (2020) 1, Приложение, пункт A.7. В уже вынесенном решении о системе SyRi для обнаружения мошенничества Окружной суд Гааги отметил, что «с учетом больших объемов данных, которые могут обрабатываться в SyRi, включая специальные персональные данные, и того обстоятельства, что используются профили рисков», был «риск того, что SyRi непреднамеренно» создаст связи, основанные на предвзятости, например, связанные с иммиграционным прошлым (параграф 6.93). Суд также отметил, что анализ больших наборов данных может привести к «нежелательным результатам, включая неоправданное исключение или дискриминацию» (параграф 6.91), и повторил мнение, поддержанное Специальным докладчиком ООН по вопросу о крайней бедности и правах человека Филипом Алстоном, по словам которые СИРИ оказали дискриминационный и стигматизирующий эффект, распространив негативные стереотипы на всех жителей районов, исследованных как проблемные (параграф 6.92). Олстон действительно серьезно беспокоило то, что система на самом деле нацелена на бедные районы в Нидерландах, сосредоточив внимание на их жителях без каких-либо конкретных подозрений в совершении индивидуальных правонарушений (Пресс-служба независимых экспертов по правам человека ООН, 2020).

[155] См. Также: Министерство юстиции США, 2014 г., стр. 22 («Точно так же продолжительность тюремного заключения подсудимого не должна корректироваться просто потому, что статистический анализ показал, что другие преступники с аналогичными демографическими профилями, скорее всего, совершат преступление в будущем. Вместо этого принцип равной справедливости требует, чтобы определение приговора основывалось в первую очередь на собственном поведении обвиняемого и криминальное прошлое»).

производства данных и повышают риск создания неточных, искаженных или систематически предвзятых данных («грязные данные») (Richardson, Schultz & Crawford, 2019, 192)[156]. Авторы указали, что «прогнозирующая полицейская деятельность» опирается на исторические данные о преступности риск разжигать цикл искаженного правоприменения: как подчеркнули криминологи, отчеты о преступлениях и статистика, собранная полицией, частично являются отчетом о реакции правоохранительных органов на то, что происходит в сообществе, и не обязательно точным отчетом обо всех преступлениях, совершенных в указанном сообщества (Robinson & Koepke, 2016). Даже «системы прогнозирования», которые не используют никаких личных данных, могут иметь негативное влияние. Например, «прогнозы рисков, связанных с местоположением», могут привести к экстренным полицейским проверкам в определенных районах, определенных как горячие точки, и, следовательно, на этническое или социальное профилирование групп населения, проживающих там (Datenethikkommission, 2019, 215).

В разделе «Общие выводы» Постановления о прекращении тайного наблюдения, запрещающего определенные виды использования распознавания лиц в Сан-Франциско, отмечается, что «хотя технология наблюдения может угрожать конфиденциальности всех нас, слежка исторически использовалась для запугивания и подавления определенных сообществ и групп» чем другие, в том числе те, которые определяются общей расой, этнической принадлежностью, религией, национальным происхождением, уровнем дохода, сексуальной ориентацией или политической перспективой»[157].

В отношении вопросов недискриминации и равенства Комиссар Совета Европы по правам человека заявил, что «государства-члены должны применять высочайший уровень контроля при использовании ИИ системы в контексте правоохранительной деятельности, особенно при использовании таких методов, как упреждающая или превентивная работа полиции» (Комиссар Совета Европы по правам человека, 11). Комиссар утверждает, что «такие системы необходимо подвергнуть независимой проверке перед развертыванием на предмет наличия любого дискриминационного эффекта, который может указывать на фактическое профилирование конкретных групп», и что «если такие эффекты обнаружены, система не может использоваться».

---

[156] Как следствие, системы, основанные на таких данных, будут проблематичными, если они не будут предлагать технические меры безопасности для адекватного смягчения или разделения «грязных данных», технические меры безопасности, которые, согласно их анализу, не доказано, что оно существует (Richardson, Schultz & Crawford, 2019, 226). Таким образом, исследователи подчеркнули необходимость разработки надежных механизмов для оценки вреда, связанного с использованием исторических данных полиции, «подкрепленных строгими мерами общественной прозрачности и подотчетности» (то же самое).

[157] Постановление о прекращении тайного наблюдения, раздел 1, § c.

Предвзятость и дискриминация могут проявляться на многих уровнях в системах ИИ[158]. Исследования показали, например, что коммерческие продукты, классифицирующие людей на мужчин и женщин с использованием алгоритмов автоматического анализа лица, страдают от существенных различий в точности в зависимости от цвета лица человека, кожа и их настоящий пол, причем темнокожие женщины являются наиболее ошибочно классифицируемой группой (Buolamwini and Gebru, 2018).

В Белой книге Европейской комиссии по ИИ дискриминация по признаку пола упоминается как один из основных потенциальных рисков, связанных с ИИ (COM (2020) 65 final, 1), и выдвигается в качестве возможного требования по снижению этого риска установление «особых обязательств перед использовать наборы данных, которые являются достаточно репрезентативными, особенно для обеспечения того, чтобы все соответствующие аспекты пола, этнической принадлежности и других возможных оснований для запрещенной дискриминации надлежащим образом отражались в этих наборах данных» (там же 19). Однако нельзя предотвратить или смягчить алгоритмическую дискриминацию только за счет регулирования наборов данных или поощрения разнообразия в областях, связанных с ИИ[159], так как это также может быть вызвано дизайном алгоритмов или дизайном системы, реализующей его.

В отношении дискриминации по признаку пола[160] крайне важно отметить, что, хотя в законе ЕС о защите данных есть особые правила, ограничивающие автоматизированное принятие индивидуальных решений на основе «конфиденциальных данных»[161], понятие охватывает различные категории

---

[158] Общепризнано, что во многих случаях «компьютерная дискриминация не основывается на использовании явно дискриминационных критериев» (Korff, 2012, 22), а скорее «проникает в алгоритмы гораздо более коварными способами» (там же, 23).

[159] В своем Коммюнике 2019 года о создании доверия к искусственному интеллекту, ориентированному на человека, Европейская комиссия отметила, что гендерное разнообразие «должно обеспечиваться на каждом этапе развития ИИ» (COM (2019) 168 final, 2).

[160] Что касается гендерной дискриминации, Белая книга по ИИ относится к подготовке Консультативным комитетом ЕС по равным возможностям для женщин и мужчин заключения по искусственному интеллекту (там же, 11), документ, который к тому времени уже был опубликован (Консультативный комитет по вопросам равных возможностей для женщин и мужчин, мнение об искусственном интеллекте, 2020 г.). Это Мнение подчеркивает важность предмета, но продвигается в качестве основной рекомендации для (дальнейшего) «отражения и анализа
на уровне ЕС и государств-членов, приспособлена ли существующая законодательная и институциональная база
к решению возникающих юридических вопросов, связанных с ИИ и гендерной эгидой и недискриминации или есть ли необходимость в реформе в общих рамках для поощрения и защиты прав человека» (там же, 6). В этом контексте это, в частности, ссылается на работу Группы экспертов высокого уровня по ИИ, и конкретно его рекомендаций по вопросам политики и инвестиций для Благонадежный AI, документ, в первую очередь, сопоставляющего гендерные вопросы необходимости решать проблему гендерного разрыва в цифровых навыков
по улучшению образования (AI HLEG, 2019b, 32-35). Для более детального обсуждения проблем искусственного интеллекта и право ЕС, см. автор: Gonzalez Fuster, 2020.

[161] Статья 9 (1) GDPR перечисляет особые категории данных (часто называемых «конфиденциальными данными», как в Рекитале (10) GDPR): «Обработка персональных данных, раскрывающих расовое или

данных, часто используемых как дискриминационная практика, эти правила защиты данных о «особых категориях данных» не распространяются на данные о поле. Действительно, гендерная принадлежность не является категорией данных, которые, согласно закону ЕС о защите данных, заслуживают особой защиты как «особая категория данных»[162], и это несмотря на то, что существует широкий консенсус относительно реальности связанных с ИИ гендерных дискриминация[163].

4.5 Право на эффективное средство правовой защиты и на справедливое судебное разбирательство

Технологии, связанные с искусственным интеллектом, могут повлиять на эффективные средства правовой защиты в основном двумя способами:

во-первых, они могут изменить характер решений, которые могут быть оспорены людьми, создавая новые проблемы;

во-вторых, они могут повлиять на то, как люди могут фактически оспаривать решения, через судебную систему. В первом случае речь идет, например, о возможности оспаривания такой меры, как вмешательство правоохранительных органов, основанное на распознавании лиц или существенно пострадавшее от него (EU FRA, 2019, 31). Последнее касается развития ИИ в самой системе правосудия.

Необходимость поддерживать ИИ «под контролем человека» часто упоминается в политических дискуссиях и в литературе в этой области. Сделать этот контроль видимым имеет значение с точки зрения прояснения того, кто несет ответственность за нарушения основных прав.

Комиссар Совета Европы по правам человека «подчеркнул в этом смысле, что «государства должны установить четкие границы ответственности за нарушения прав человека, которые могут возникнуть на различных этапах

этническое происхождение, политические взгляды, религиозные или философские убеждения или членство в профсоюзах, а также обработка генетических данных, биометрических данных с целью однозначной идентификации физического лица, данных, касающихся здоровья, или данных, касающихся половой жизни или сексуальной ориентации физического лица, запрещены».

[162] Можно утверждать, что определенные методы обработки данных, которые могут привести к дискриминации по признаку пола, будут нарушать определенные принципы обработки данных, такие как принцип справедливости согласно GDPR. Изложение (71) GDPR провозглашает, что «для обеспечения справедливой и прозрачной обработки» контролер должен «защищать личные данные таким образом, чтобы учитывать потенциальные риски, связанные с интересами и правами субъекта данных, и предотвращать, среди прочего, дискриминационные последствия для физических лиц по признаку расового или этнического происхождения, политических убеждений, религии или убеждений, членства в профсоюзах, генетического статуса или состояния здоровья или сексуальной ориентации, или которые приводят к мерам, имеющим такой эффект».

[163] В этом смысле, например: КОМЕСТ, 2019, 21.

жизненного цикла системы искусственного интеллекта» (Комиссар Совета Европы по правам человека, 2019 г., стр. 13). Комиссар также отметил, что «никому, кто утверждает, что он является жертвой нарушения прав человека, возникшего в результате разработки, развертывания или использования государственным или частным лицом системы ИИ, не должно быть предоставлено эффективное средство правовой защиты в национальном органе власти», добавив, что «государства должны предоставить доступ к эффективным средствам правовой защиты тем, кто подозревает, что они подверглись действию меры, которая была полностью или в значительной степени проинформирована о результатах работы системы ИИ непрозрачным образом и без их ведома» (то же самое).

Использование систем искусственного интеллекта в области правоприменения и уголовного правосудия, как правило, может вызывать озабоченность в отношении стандартов справедливого судебного разбирательства, предусмотренных статьёй 6 ЕКПЧ, в частности, презумпции невиновности, права быть незамедлительно проинформированным о причине и характере обвинение, право на справедливое судебное разбирательство и право защищать себя лично (MSI-NET, 201 8, 10)[164]. Возможное использование алгоритмических систем в контексте правосудия было выделено как сектор, в котором эти системы противоречат конституционно защищенным правам первостепенной важности, что означает, что их использование может, независимо от возможных защитных мер, быть разрешено только в ограничительных условиях или запрещено (Datenethikkommission, 2019, 212). В этом смысле даже юридически необязательные предложения о вынесении решений алгоритмическими системами обычно следует рассматривать как весьма проблематичные с точки зрения заинтересованных сторон (там же, 213).

Права ребенка

Хартия ЕС об основных правах посвящает правам ребенка специальное положение (статья 24), что не означает, что дети не пользуются, кроме того, всеми другими основными правами, закрепленными в Хартии ЕС, такими как, например, право на защиту персональных данных. ЕСПЧ подчеркнул, что сохранение государственными органами данных, касающихся невиновных лиц,

---

[164] Связанные опасения могут возникнуть в отношении статьи 5 ЕКПЧ, защищающей от произвольного лишения свободы, и статьи 7 (нет наказания без закона) (MSI-NET, 2018, 10). Подчеркивая, что использование ИИ в судебных системах может потенциально нарушить право на справедливое судебное разбирательство, в частности, право на естественное судебное разбирательство, установленное законом, право на независимый и беспристрастный суд и равноправие судебных разбирательств: Ronsin & Lampos, 2018, 11.

«может быть особенно вредным в случае несовершеннолетних», «учитывая их особое положение и важность их развития и интеграции в общество»[165].

Есть несколько случаев, в которых несовершеннолетние появляются в виде прямой или косвенной цели АИ-связанные инициатив в области правоохранительных органов[166]. Главным образом соответствующие проблемы выдают сбор данных о несовершеннолетних по отношению к границам. Что касается обработки данных граждан третьих стран и автоматизированной оценки, связанных с ними рисков, было указано, что уязвимые группы, включая беженцев, сталкиваются с уникальными рисками в случае, если информация о них достигнет репрессивных правительств в их странах, которые могут превратить данные в оружие, подвергая людей и их семьи серьезному личному риску (Molnar & Gill, 2018, 43).

Такие события, как более широкое участие несовершеннолетних в демонстрациях, особенно в связи с изменением климата (среди прочего, вслед за активисткой Гретой Тунберг), вызывают важные вопросы о том, как конкретно защитить их права перед лицом наблюдения за такими событиями демонстрации, но также и в отношении возможного онлайн-наблюдения за соответствующей онлайн-деятельностью организации.

В Рамках ответственных ограничений на распознавание лиц ВЭФ прямо упоминает права детей (WEF, 2020). В нем говорится, что, хотя распознавание лиц никого не должно исключать и всегда должно быть доступно и использоваться всеми группами людей, «могут быть некоторые случаи, такие как младенцы и дети, в которых уместно исключение из этого принципа и альтернатива ему должна быть предложена идентификация лица» (там же, 9).

Согласно EU FRA, одна из возможностей распознавания лиц в правоохранительных органах - это использовать его для поиска пропавших без вести детей (EU FRA, 2019, 18). Однако очень неясно, как можно использовать распознавание лиц для таких целей без несоразмерного нарушения основных прав всех детей.

5. Разработка политики

В этом разделе представлены соответствующие политические соображения, касающиеся регулирования ИИ, с упором на обсуждения на

---

[165] Марпер против Соединенного Королевства, решение от 4 декабря 2008 г., заявления 30562/04 и 30566/04, ECLI: CE: ECHR: 2008: 1204JUD003056204, параграф 124.

[166] Тот факт, что данные о несовершеннолетних могут появиться в базах данных правоохранительных органов, используемых для оценки риска, уже указывался выше в связи с делом о матрице насилия между бандами (GVM).

уровне ЕС, но помещены их в более широкий контекст, в частности, со ссылкой на события Совета Европы. Европейские политические инициативы многочисленны, и подробный анализ всех их выходит за рамки настоящего исследования[167]. Европейские инициативы вписываются в еще более богатый контекст глобальных инициатив и дебатов вокруг ИИ[168], которые могут быть политическими дебатами, но также иногда заметно более технический и академический[169].

Международные инициативы с упором на искусственный интеллект, правоохранительную деятельность и уголовное правосудие встречаются сравнительно реже, чем другие. Инновационный центр Интерпола и Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия (ЮНИКРИ) создали Центр искусственного интеллекта и робототехники и созвали глобальное совещание по этой теме в 2018 году, в результате чего в 2019 году был опубликован отчет (Интерпол и ЮНИКРИ, 2019). В отчете отмечалось, что многие страны уже тогда изучали применение ИИ и робототехники в контексте правоохранительной деятельности, призывая к обсуждению их этического использования и социального воздействия (там же, vi).

Инициативы, исходящие от Совета Европы, многочисленны. В 2017 году Парламентская ассамблея Совета Европы (ПАСЕ) приняла Рекомендацию о технологической конвергенции, искусственном интеллекте и правах человека, в которой, в частности, предлагалось составить руководящие принципы «общей системы стандартов, которые должны соблюдаться, когда суд использует искусственный интеллект» (пункт 9.2).

В 2018 году Европейская комиссия по эффективности правосудия (CEPEJ) приняла Европейскую этическую хартию по использованию ИИ в

---

[167] В рамках базового исследования проекта Агентства «Искусственный интеллект (ИИ), большие данные и основные права» FRA ЕС собрало информацию об инициативах в области политики, связанных с ИИ, в государствах-членах ЕС и за его пределами в период с 2016 г. 2020. Коллекция на данный момент включает более 290 инициатив. «Политическая инициатива» получила широкое определение, чтобы включать в себя ряд инициатив, которые потенциально могут способствовать выработке политики и установлению стандартов в области искусственного интеллекта. Это может быть, среди прочего, действующий (проект) законодательства, мягкое право, руководящие принципы и рекомендации по использованию ИИ или отчеты, содержащие выводы, имеющие политическое значение. Гражданское общество также внесло свой вклад в дебаты о регулировании ИИ ЕС. Access Now Europe, например, в 2019 году подчеркнула, что ЕС должен обеспечивать соблюдение и развивать самые высокие стандарты соблюдения прав человека для новых технологий и систем искусственного интеллекта, которые спроектированы, разработаны или развернуты на его территории (Access Now Europe, 2019, 5), и выдвинул ряд рекомендаций.

[168] В качестве иллюстрации глобального интереса к этой проблеме Организация экономического сотрудничества и развития (ОЭСР) приняла в 2019 году свои Принципы в отношении ИИ. Другой пример: в США в 2016 году Управление науки и технологий Белого дома Обамы выступило с инициативой «Подготовка к будущему искусственного интеллекта», посвященной рискам и преимуществам ИИ. Больше информации на сайте инициативы.

[169] Объединение, например, вокруг ключевых слов «Справедливость, подотчетность и прозрачность» (FAT).

судебных системах и их среде (CEPEJ, 2018), ориентированную на государственные и частные заинтересованные стороны, ответственные за разработку и внедрение ИИ инструменты и услуги, которые включают обработку судебных решений и данных, а также лиц, принимающих решения, отвечающих за законодательную или нормативную базу, за разработку, аудит или использование таких инструментов и услуг. Хартия выдвигает пять принципов: уважение основных прав; недискриминации; качества и безопасности; прозрачности, беспристрастности и справедливости; и «под контролем пользователя» (там же, 5).

В этической хартии CEPEJ отмечается, что обработка судебных решений ИИ может в гражданских, коммерческих и административных делах помочь повысить предсказуемость применения закона и последовательность судебных решений, но что в уголовных делах его использование должно рассматриваться с величайшими оговорками в целях предотвращения дискриминации на основе конфиденциальных данных в соответствии с гарантиями справедливого судебного разбирательства» (там же, 4)[170].

Комиссар Совета Европы по правам человека опубликовал в 2019 году Рекомендацию под названием «Распаковка искусственного интеллекта: 10 шагов по защите прав человека», в которой описывается ряд шагов для национальных властей по максимальному использованию потенциала ИИ при одновременном предотвращении или смягчении негативного воздействия на жизнь людей и права (Комиссар Совета Европы по правам человека, 2019). Он фокусируется на 10 ключевых областях деятельности: оценка воздействия на права человека, общественные консультации, стандарты прав человека в частном секторе, информация и прозрачность, независимый надзор, недискриминация и равенство, защита данных и конфиденциальность, свобода выражения мнений, свобода собраний ассоциации и право на труд; доступ к средствам правовой защиты; и продвижение грамотности в области ИИ. Последнее прямо связано с необходимостью распространения знаний и понимания ИИ «в государственных учреждениях, независимых надзорных органах, национальных структурах по правам человека, судебных и правоохранительных органах», а также среди широкой общественности[171].

---

[170] Что касается гражданских, коммерческих и административных вопросов, исследование, сопровождающее Хартию, выделяет среди основных гарантий, которые должны быть подтверждены, право на доступ к суду, принцип состязательности, равенство сторон, беспристрастность и независимость судей и право на адвоката (Ronsin & Lampos, 2018, 34-35).

[171] Рекомендация «Распаковка искусственного интеллекта» также содержит контрольный список, который поможет реализовать меры, рекомендованные в каждой ключевой области. Что касается доступа к средствам правовой защиты, то к ним можно отнести необходимость оценки того, предоставляют ли законы «эффективное средство правовой защиты тем, кто утверждает, что является жертвой нарушения прав человека, возникшего в результате разработки, развертывания или использования системы искусственного интеллекта», необходимость «обеспечить, чтобы режимы ответственности четко устанавливали, кто несет юридическую ответственность за весь спектр нарушений прав человека, которые могут происходить на каждом этапе

В апреле 2020 года Комитет министров Совета Европы принял Рекомендацию о воздействии алгоритмических систем на права человека[172], в том числе Руководящие принципы по устранению воздействия алгоритмических систем на права человека. Руководство предназначено для консультирования государств, а также субъектов государственного и частного секторов во всех их действиях, касающихся проектирования, разработки и текущего развертывания алгоритмических систем, которые, как отмечается в документе, часто «не являются ни однозначно публичными, ни явно частными»[173]. Обеспечивать эффективную защиту прав человека и основных свобод всех людей на протяжении всего технологического развития, государства «должны воздерживаться от нарушения прав человека посредством использования алгоритмических систем и должны разработать законодательную и нормативную базу, способствующую созданию среды, в которой все участники уважают и продвигать права человека и стремиться предотвращать возможные нарушения»[174].

В этих Руководящих принципах 2020 отмечается, что алгоритмические системы иногда «используются в целях прогнозирования в контексте полицейской деятельности и пограничного контроля, в целях борьбы с отмыванием денег и мошенничеством»[175]. Они отмечают, что определенные приложения алгоритмических систем «могут побуждать к определенным, более высоким риск для прав человека», например, если они используются государствами для их государственной службы или реализации государственной политики. Подобный повышенный риск, поясняется в Руководстве, «возникает в результате использования в контексте процессов принятия решений государственными органами или частными сторонами в ситуациях, которые имеют особый вес или юридическое обоснование», и, следовательно, использования алгоритмических Системы в судебной сфере для целей правового анализа, прогнозирования или оценки индивидуального риска должны вводиться с большой осторожностью и в соответствии с гарантиями

жизненного цикла системы ИИ», а также «гарантировать, что судебная система и другие соответствующие национальные органы не будут придавать несоответствующее значение предполагаемой / воспринимаемой точности или объективности системы ИИ и обеспечивать равенство сторон между жертвой и обвиняемым в делах, оспаривающих нарушения прав человека, вызванные системами ИИ» (Комиссар по правам человека Совета Европа, 2019, 23).

[172] Рекомендация CM / Rec (2020)1 Комитета министров государствам-членам о воздействии алгоритмических систем на права человека, принятая Комитетом министров 8 апреля 2020 года на 1373-м заседании заместителей министров.

[173] Приложение, п. A.12.

[174] Приложение, п. A.1. Конкретно в качестве первого шага. Государства должны пересмотреть свои законодательные основы и политику, а также свои собственные практики в отношении закупок, проектирования, разработки и постоянного развертывания алгоритмических систем и убедиться, что они соответствуют представленным Руководящим принципам (Рекомендация, параграф 1).

[175] Приложение, п. A.8.

справедливого судебного разбирательства в статье 6 ECHR[176]. Термин «высокий риск» вводится в этом контексте для обозначения «использования алгоритмических систем в процессах или решениях, которые могут привести к серьезным последствиям для людей, или в ситуациях, когда отсутствие альтернатив вызывает особенно высокую вероятность нарушения прав человека, в том числе путем введения или усиления несправедливости при распределении доходов»[177].

По-прежнему в контексте Совета Европы работа над отчетом о правосудии по алгоритму: роль искусственного интеллекта в полицейской деятельности и системах уголовного правосудия была начата после предложения, внесенного Комитетом по юридическим вопросам и правам человека Парламентской ассамблеи в 2018 году. (PACE)[178]. Специальный комитет Совета Европы по ИИ (САНИИ) был создан с целью изучения целесообразности, осуществимости и потенциальных элементов правовой основы для разработки, проектирования и применения ИИ. ЕС вносит свой вклад в САНИИ в качестве наблюдателя.

5.1 Вступление

Последние годы были особенно богаты политическими разработками на уровне ЕС, явно связанными с ИИ. Особенно с 2018 года институты ЕС очерчивают контуры того, что все больше принимает форму повестки дня в области ИИ[179]. В этом подразделе более подробно рассматривается вклад в такие дебаты по ИИ со стороны Европейской комиссии и Европейского парламента[180], а также специальные гранты внимание к роли этики и финансированию ИИ в этом контексте.

Ряд других разработок на уровне ЕС, формально не связанных с обсуждениями политики в области ИИ, можно рассматривать как потенциально

---

[176] Там же, пункт A.11.

[177] То же. В Руководстве утверждается, что «Государства должны применять предупредительный подход и требовать отказа от определенных систем, если их развертывание приводит к высоким рискам необратимого ущерба или когда из-за их непрозрачности человеческий контроль и надзор становятся непрактичными» (Там же, параграф A.15).

[178] Ходатайство о вынесении рекомендации Правосудие по алгоритму - роль искусственного интеллекта в полицейской деятельности и системах уголовного правосудия, Док. 14628, 26 сентября 2018 г.

[179] В том смысле, что это не отличалось от постепенного появления, объединения единого цифрового рынка и политики безопасности, повестки дня и политики ЕС в области кибербезопасности.

[180] Другие учреждения EU также играют важную роль в этой области. В феврале 2019 года Совет принял выводы
по ИИ, призывающие к «более активной разработке, развертыванию и внедрению приложений искусственного интеллекта во всех секторах экономики с целью сделать Европу мировым лидером в области искусственного интеллекта», подчеркнув при этом «необходимость создания соответствующих требования кибербезопасности для
ИИ и обеспечения подотчетности и защиты основных прав» (Совет ЕС, 6177/19, 7 и 8).

значимое влияние на влияние ИИ на основные права ЕС в области правоохранительной деятельности и уголовного правосудия. В целом следует отметить, что за последние годы AFSJ стал свидетелем серьезных преобразований в способах обработки данных. Этот переход был описан как переход от «разрозненного подхода», при котором разные информационные системы работают как отдельные объекты и где решающее значение имеет строгая интерпретация принципа ограничения цели, к новому подходу, в котором ключевым словом является функциональная совместимость. Как правило, данные, изначально обработанные не в правоохранительных целях, могут быть доступны для обработки правоохранительными органами. Положение Европола, пакет совместимости и Регламент ETIAS были выделены в качестве примеров этой тенденции (Coudert, 2017).

Что касается распознавания лиц, особенно актуальным является интерес к распознаванию лиц в контексте Prium Decision[181], основанного на принципе международного поиска. Приурочив к 10-летнему юбилею Prum, Совет призвал экспертов государств-членов «оценить рабочий процесс Prum для дальнейших разработок с точки зрения возможных новых биометрических технологий, например, систем распознавания лиц» (Генеральный секретариат Совета, 2018). Некоторые частично общедоступные документы[182] перекликаются с созданием Оперативной группы по распознаванию лиц, связанной с Рабочей группой Совета по распознаванию лиц обмен информацией и защита данных (DAPIX) (Председательство в Совете, 2019 г.). Другие документы свидетельствуют о рассмотрении указанной фокус-группой предварительных результатов технико-экономического обоснования внесения поправок в действующее законодательство Prum, исследования, проведенного консалтинговой фирмой от имени Европейской комиссии, которая предположительно представила в качестве предложения возможность создания центральной базы данных для распознавания лиц в ЕС - предложение, тем не менее, отклонено экспертами Оперативной группы, в частности, из-за отсутствия у него операционных преимуществ (Austrian Delegation to the Council, 2019, 9).

Некоторые исследования, финансируемые ЕС, уже продвигаются в этом направлении.[183] Проект «На пути к европейскому уровню обмена изображениями лиц» (TELEFI)[184], согласно его веб-сайту, проводит

---

[181] Решение Совета 2008/615/JHA от 23 июня 2008 г. об активизации трансграничного сотрудничества, особенно
в борьбе с терроризмом и трансграничной преступностью, OJL 210, 6.8.2008, с. 1-11. Prtim - одна из инициатив EU AFSJ по обработке данных, которая с самого начала открыто посвящена обработке данных в правоохранительных целях, основанной на разработке децентрализованных инструментов для обмена информацией.

[182] Доступная общедоступная информация об этих разработках ограничена, и некоторые доступные сведения связаны с утечками (см., например, Campbell and Jones, 2020).

[183] Как указано, например, в: Monroy, 2020.

[184] Финансирование через Фонд внутренней безопасности Европейского Союза - Полиция (Соглашение о

исследование того, как распознавание лиц в настоящее время используется для исследования преступности в странах-членах ЕС, уделяя особое внимание «возможности осуществления обмена изображениями лиц в рамках Prum». В рамках проекта основное внимание уделяется использованию распознавания лиц в уголовных расследованиях, но в настоящее время проводятся исследования различных баз данных, чтобы в будущем «рассмотреть возможность использования этих дополнительных баз данных на законных основаниях для уголовных расследований/разбирательств и транснациональных расследований обмен данными»[185].

5.2. Европейская комиссия

До сих пор разработки, связанные с искусственным интеллектом, в основном фигурировали в дискуссиях о едином цифровом рынке[186]. В своей Рабочей программе на 2018 год Европейская комиссия объявила под заголовком «Объединенный единый цифровой рынок» о своем стремлении «максимально использовать возможности искусственного интеллекта будет все больше играть роль в наших экономиках и обществах» (COM (2017) 650 final, 5)[187]. В Рабочей программе на 2020 год под заголовком «Европа, пригодная для цифровой эпохи» Комиссия объявила о своем намерении выдвинул Белую книгу по искусственному интеллекту «в поддержку его разработки и внедрения и обеспечения полного уважения европейских ценностей и основных прав» с учетом «максимального использования искусственного интеллекта» при создании «экосистемы доверия для обеспечения он развивается в четко определенных этических границах» (COM (2020) 37 final, 4). Создание «подключенной цифровой единой маркировки» было одним из приоритетных направлений деятельности полиции Жан-Клода Юнкера (Juncker, 2014, стр. 6); единый цифровой рынок был определен как «рынок, на котором

гранте: 821284), срок действия с января 2019 года по сентябрь 2020 года; больше информации на сайте TELEFI.

[185] См. «О проекте TELEFI».

[186] Участие Европейской комиссии в поддержке политики в области ИИ и ИИ включает в себя множество инициатив. Например, это принимает и поддерживает Европейский альянс искусственного интеллекта, где представители бизнеса, потребительских организаций, профсоюзов и другие представители органов гражданского общества должны взаимодействовать с экспертами (AI HLEG) в формате форума и кормить в диалог с заинтересованными сторонами. Кроме того, после призывов Европейского парламента Европейской комиссией был заказан пилотный проект по повышению осведомленности об алгоритмах, который был активен в 2018 году (см. Веб-сайт: https://algoaware.lpweb.eu/). В 2018 году Европейская комиссия запустила AI Watch, службу знаний для мониторинга развития, внедрения и воздействия ИИ в Европе. AI Watch поддерживается Объединенным исследовательским центром (JRC) Европейской комиссии в сотрудничестве с Генеральным директоратом коммуникационных сетей, контента и технологий (DG CONNECT). AI Watch объявила, что отслеживает также использование и влияние технологий искусственного интеллекта, используемых в государственных службах и в общественных организациях.

[187] В Рабочей программе на 2019 год под тем же названием отмечалось, что Европейская комиссия продолжит «работу над возникающей проблемой искусственного интеллекта, обеспечивая скоординированные действия во всех европейских странах» (COM (2018) 800 final, 3).

обеспечивается свободное передвижение товаров, людей, услуг и населения» (COM (2015) 192 final, 2)[188].

Это лишь некоторые из основных моментов в довольно долгой истории поддержки Европейской комиссией обработки данных как ключевого фактора роста европейской экономики, истоки которого восходят к 1970-м годам[189]. 2018 год был особенно плодотворным по отношению к политике ИИ. Европейская комиссия опубликовала сообщение, охватывающее понятие «человеко-ориентированный ИИ» и трехсторонний подход к увеличению технологического и промышленного потенциала ЕС и его распространения в экономике; подготовиться к социально-экономическим изменениям и обеспечить соответствующую этическую и правовую базу (COM (2018) 237 final). Комиссия также разработала совместно с государствами-членами скоординированный план по ИИ для создания синергизма, объединения данных и увеличения совместных инвестиций (COM (2018) 795 final).

Даже если раньше термин ИИ как таковой не был особенно заметен, существует явная преемственность с предыдущими дискуссиями о «больших данных». В своем сообщении 2014 года о процветающей экономике, основанной на данных, Европейская комиссия описала «большие данные» как относящиеся к «большим объемам различных типов данных, производимых с высокой скоростью из большого количества различных типов источников», и отметила, что обработка такие данные требовали «новых инструментов и методов, таких как мощные процессоры, программное обеспечение и алгоритмы» (COM (2014) 442 final, 4), отмечая также наступление «новой промышленной революции, основанной на цифровых данных, вычислениях и автоматизации» (там же, 2).

В отчете 2019 г., посвященном созданию доверия к человеко-ориентированному искусственному интеллекту, «доверие», упомянутое в названии, было открыто связано Европейской комиссией в первую очередь с тестированием «практической реализации этических рекомендаций по разработке и использованию ИИ» (COM (2019) 168 финал, 1). ЕС заявил, что приложения ИИ «должны не только соответствовать закону, но и соответствовать этическим принципам» и уважать основные права граждан. Точные отношения между этими идеями не были четко определены, но

---

[188] Он расширил тот факт, что уже в 1995 году законодатель ЕС установил принцип свободного перемещения персональных данных внутри ЕС (Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физическим лицам в отношении обработки персональных данных и свободного перемещения таких данных, OJL 281, 23.11.1995, стр. 31-50), в частности, чтобы в 2018 году установить свободное перемещение неличных данных.

[189] Уже тогда, когда Европейская комиссия очертила контуры своей основополагающей политики Сообщества в отношении данных, она отметила, однако, что разрабатываемые «банки данных» могут содержать полицейские данные и, следовательно, правила доступа к таким данным информация была «жизненно важной» (SEC (73) 4300 final, 13).

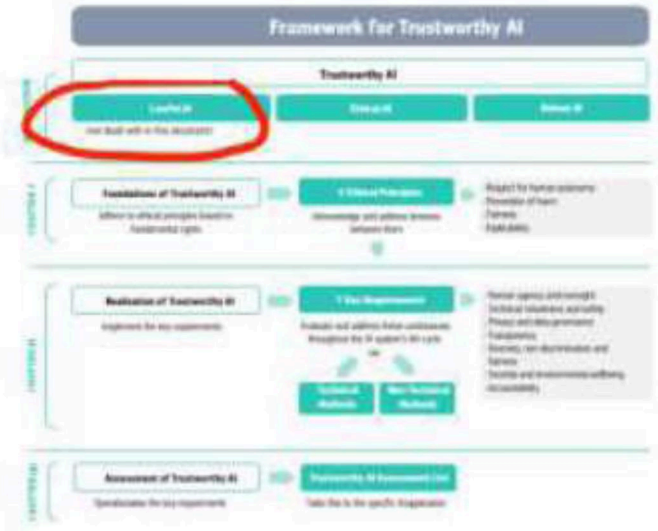
предполагаемый пункт действий заключался в том, что «необходимы этические руководящие принципы, основанные на существующей нормативной базе», поэтому ЕК учредила Группу экспертов высокого уровня поручено разработать такие руководящие принципы (COM (2019) 168 final, 2).

Группа экспертов высокого уровня по искусственному интеллекту (ИИ HLEG) представила в 2018 году первый проект своих Руководящих принципов этики в области искусственного интеллекта и опубликовала пересмотренный документ в 2019 году после открытой консультации, которая вызвала обширные отзывы (ИИ HLEG, 2019a). В Руководстве по этике ИИ HLEG по ИИ перечислены требования к «заслуживающим доверия» системам ИИ, требования, которые были проверены в ходе пилотного процесса, который, как ожидается, завершится публикацией еще одного измененного документа в 2020 году.

Роль, отведенная закону и основным правам в Руководстве по этике ИИ HLEG, относительно неуловима и потенциально вводит в заблуждение. ИИ HLEG действительно заявляет, что «заслуживающий доверия ИИ» должен быть законным, этичным, надежным, но отмечает, что его Руководящие принципы по этике «прямо не затрагивают» компонент законности заслуживающего доверия ИИ, предпочитая вместо этого предлагать рекомендации по компонентам этики и надежности. (ИИ HLEG, 2019a, 2). В сноске далее разъясняется, что заявления Руководства «не предназначены для предоставления юридических консультаций или рекомендаций по соблюдению применимого законодательства», но в то же время признается, что «многие из этих заявлений в некоторой степени уже отражены в существующие законы» (то же самое). Далее в документе другая сноска настаивает на том, что он «не дает никаких рекомендаций по обеспечению соблюдения правовых норм (законный ИИ)» (там же, 3). На рисунке ниже показано, как ИИ HLEG открыто заявляет о необходимости отложить в сторону соображения законности в отношении ИИ.

IPOL | Policy Department for Citizens' Rights and Constitutional Affairs

Figure 2: AI HLEG Framework for Trustworthy AI



Источник: рисунок из ИИ HLEG, 2019a, 8. Обведено красным цветом автором этого исследования.

Итак, нет реальных субстантивных обоснований в HLEG Руководстве ИИ самим по себе почему эта группа не будет уделять никакого внимания требованиям «законного ИИ». Как-то загадочно, та же группа экспертов настаивает на том, что «заслуживающий доверия ИИ» будет иметь решающее значение для использования преимуществ ИИ «таким образом, чтобы это соответствовало нашим основополагающим ценностям уважения прав человека, демократии и верховенства закона» (ИИ HLEG, 2019a, 4). Что еще более сбивает с толку, в том же документе «Руководящие принципы этики» в конечном итоге объявляется, что он «не должен вкратце касаться требований «законного ИИ», только для того, чтобы отметить, что он исходит из предположения, что все соответствующие юридические права и обязанности, которые не подробно описаны, «остаются обязательны и должны должным образом соблюдаться» и что полная реализация этичного и надежного ИИ может (или не может) «выходить за рамки существующих юридических обязательств» (там же, 6), какими бы они ни были.

Тем не менее, наиболее неоднозначным выбором Руководства по этике, вероятно, является отождествление того, что называется «основами надежного ИИ» с «подходом, основанным на фундаментальных правах» (ИИ HLEG, 2019a, 7). Такое предложение сопровождается сноской, в которой утверждается, что основные права что юридически осуществимые права, гарантируемые

договоров ЕС и Хартии ЕС»[190], и в качестве такого элемента «законного ИИ» в той степени, что они являются юридически обязательными. Однако в сноске утверждается, что основные права могут «также пониматься как отражающие особые моральные права всех людей, возникающие в силу их человечности, независимо от их юридически обязательного статуса», и в этом смысле они также являются частью «этического ИИ» (то же). В качестве неизбежного логического следствия следует понимать, что всякий раз, когда ИИ HLEG ссылается на основные права, он может или не может ссылаться на права, которые являются юридически обязательными. В той степени, в которой он открыто утверждает, что сосредоточен на «этическом ИИ», а не на «законном ИИ», на самом деле наиболее часто основные права, обсуждаемые ИИ HLEG, не обязательно могут быть связаны с юридически обязательными правами[191], с юридической точки зрения, особенно хлопотно.

Это происходит, как на самом деле, на фон постоянной неопределенности о различии между «этическим и надежным ИИ», с одной стороны, и «законный ИИ», с другой стороны. В этом смысле семь ключевых требований, наконец выдвинутых ИИ HLEG, якобы не имеющим отношения к «законному ИИ», не лишены ссылок на правовые инструменты, такие как GDPR (ИИ HLEG, 2019a, 17). Упомянув элементарные соображения, касающиеся основ регулирования ИИ, в нескольких сносках и поддерживая почти постоянное стирание между законным и этичным, Руководящие принципы этики HLEG в области ИИ к сожалению, ни в коем случае не помогло организовать внятные политические дебаты о регулировании ИИ в ЕС и его влиянии на (юридически обязательные) основные права.

Европейская комиссия официально приветствовала работу ИИ HLEG в своем проекте по созданию доверия к человеко-ориентированному искусственному интеллекту в 2019 году, в котором, однако, не учла тот факт, что в Руководстве по этике ИИ HLEG не обсуждалось применимое право как таковое. Напротив, в соответствии с рекомендациями ЕС, руководящие принципы определили ключевые требования к «заслуживающему доверия ИИ» на основе трех его компонентов: закон, этические принципы и надежность (COM (2019) 168 final, 3). Более того, ЕС даже отметил, что многие уже существующие положения законодательства ЕС «конечно, уже отражают одно или несколько из этих ключевых требований, например, безопасность, защита личных данных, конфиденциальность» (то же самое). Это только добавило дополнительный уровень неясности в отношении того, могут ли обсуждаемые этические принципы отличаться от правовых норм и каким образом. Еще больше развлекая двусмысленность, Европейская комиссия заявила, что «этот

[190] Точная цель этого предложения, согласно которому основные права лежат в основе основных прав, установленных Хартией основных прав ЕС, остается неясной.
[191] Как это подтверждено, в частности, в AI HLEG, 2019a, 10.

ИИ является беспроигрышным предложением», связывая его с «гарантией уважения фундаментальных ценностей и прав» (COM (2019) 168 финал, 8).

В 2019 году в Союзе, который стремится к большему: моя повестка дня для Европы, тогдашний кандидат на пост президента Европейской комиссии объявила, что в течение 100 дней своего пребывания в должности президента она «предложит закон о скоординированный европейский подход к человеческим и этическим последствиям использования искусственного интеллекта» (Von der Leyen, 2019, 13). Это был ключевым элемент верхнего уровня амбиций двигаются в направлении к «Европе, пригодной для цифрового века», в том смысле, в Европе «схватив возможности с цифрового века в безопасных и этических границах». План выдвижения законодательства за 100 дней в конечном итоге превратился в разработку Белой книги. За несколько недель до публикации ходили слухи о том, что документ мог рассматриваться как возможность работы над общим запретом распознавания лиц в общественных местах, идея, которая в конечном итоге не была представлена как таковая в опубликованном документе (Yun Chee, 2020).

Европейская комиссия опубликовала свою Белую книгу по искусственному интеллекту 19 февраля 2020 года (финал COM (2020) 65). В Белой книге провозглашается, что «с учетом того серьезного воздействия, которое ИИ может оказать на наше общество, и необходимости построения доверия, жизненно важно, чтобы европейский ИИ основывался на наших ценностях и основных правах, таких как человеческое достоинство и защита конфиденциальности» (там же, 2). Будущая нормативно-правовая база для ИИ в Европе, говорится в документе, должна создать «экосистему доверия», которая представляет собой «политическую цель сама по себе» (там же, 3), которая, тем не менее, может также способствовать другим целям, таким как создание «внутренний рынок без трения для дальнейшего развития и внедрения «а также укрепление промышленной базы Европы в области искусственного интеллекта» (там же 10).

Объявленная нормативно-правовая база должна, в частности, обеспечивать «оптимальные в социальном отношении результаты и соответствие законодательству, принципам и ценностям ЕС», что «особенно актуально в областях, где права граждан» могут быть затронуты самым непосредственным образом, например, в случае приложений ИИ для правоохранительных и судебных органов» (там же, 10). Он должен быть основан на изучении того, «способно ли действующее законодательство устранить риски ИИ и может ли оно эффективно применяться, необходимы ли изменения законодательства или новое законодательство» (то же самое). Согласно Белой книге, одним из способов, которым ИИ может принести пользу Европе, является «оснащение правоохранительных органов соответствующими

инструментами для обеспечения безопасности граждан» (COM (2020) 65 final, 2).

Белая книга по ИИ была представлена вместе с двумя сообщениями, одно о формировании цифрового будущего Европы в целом, а другое конкретно о Европейской стратегии обработки данных[192]. Связь, формирующая цифровое будущее Европы, связала появление «настоящего цифрового будущего преобразование» к необходимости обеспечить безопасность цифровых приложений и продуктов, цель будет осуществляться, среди прочего, «обеспечение эффективной работы правоохранительных и судебных органов путем разработки новых инструментов борьбы с киберпреступниками» (COM (2020) 67 окончательный, 5).

В Коммюнике о европейской стратегии данных (COM (2020) 66 final) далее разрабатываются политики в отношении данных, которые на протяжении многих лет были связаны с такими понятиями, как «общее европейское пространство данных», «стратегия данных», «экономика данных», изначально «встроенная в стратегию единого цифрового рынка», а затем «примененная к ИИ» (Penner, 2019). В нем рассматриваются ограничения на свободный поток данных, включая правовые препятствия на пути к размещению данных для целей хранения и / или обработки, а также ряд вопросов, касающихся данных, таких как право собственности, доступ, повторное использование, переносимость и ответственность. Он подчеркивает ценность доступности данных (COM (2020) 66, 6). Отмечая, что данные могут использоваться «для общественного блага», в нем говорится, что данные, «созданные обществом», могут «там, где это необходимо и соразмерно, обеспечить более эффективную борьбу с преступностью» (то же самое). В рамках такой стратегии Европейская комиссия намерена профинансировать создание общих, функционально совместимых пространств данных в стратегических секторах (там же, 16), таких как «общие европейские пространства данных для государственного управления», нацеленных, в частности, на решение правовых вопросов, потребности в правоприменении и в обеспечении «инновационных» правительственных технологий, «рег-технологий» и «юридических технологий» приложений, поддерживающих практиков, а также других услуг, представляющих общественный интерес» (там же, 22).

Согласно сообщению Европейской комиссии от июня 2020 года о двухлетнем применении GDPR, Белая книга по ИИ «открыла общественные дебаты о конкретных обстоятельствах, если таковые имеются, которые могли бы оправдать использование искусственного интеллекта для целей удаленной

[192] Белая книга также сопровождалась отчетом Европейской комиссии о последствиях для безопасности и ответственности искусственного интеллекта, Интернета вещей и робототехники (COM (2020) 64 final).

биометрической идентификации (например, распознавание лиц) в общественных местах и об общих гарантиях» (COM (2020) 264 final, 10).

Реакция на Белую книгу была разной. Некоторые, например, задавались вопросом, совместима ли подтвержденная приверженность европейским ценностям с тем, чтобы идти в ногу с международными конкурентами, такими как США и Китай (Scott, 2020). Секретариат Совета Европы представил ответы на консультацию Европейской комиссии по Белой книге, в которых подчеркивалось, что «структура доверия», которая должна быть создана между всеми заинтересованными сторонами, должна иметь в качестве предварительного условия уважение нормативной базы и основных прав и значимое выполнение соответствующего действующего постановления (Секретариат Совета Европы, 2020, 5). В документе возвращается к вопросу об основных правах, чтобы заявить, что исследования, связанные с ИИ, должны «сосредоточиться на основных правах, чтобы способствовать разработке законодательства, этических стандартов и руководящих принципов по ИИ, соответствующих таким правам», и продвигать цифровые гуманитарные науки (там же, 7).

EDPS официально отреагировала на Белую книгу по ИИ 29 июня 2020 года (EDPS, Мнение 4/2020). В своем Заключении EDPS особо подчеркнула, что любая будущая нормативная база для ИИ будет применяться «как к государствам – членам ЕС, так и к институтам, офисам, органам и агентствам ЕС» (там же 2). Что касается существа, EDPS, в частности, призвала к подходу к определению уровня риска при использовании приложений ИИ, который должен быть «более надежным и более тонким» (там же, 11) в том смысле, что он должен быть многоуровневым вместо подхода «все или ничего» (там же, 13).

Заключение EDPS также поддерживает идею «моратория на развертывание в ЕС автоматизированного распознавания в общественных местах человеческих черт, не только лиц, но и походки, отпечатков пальцев, ДНК, голоса, нажатия клавиш и других биометрических или поведенческих данных сигналы» (то же самое). Мораторий должен совпадать с работой над «соответствующими гарантиями, включая всеобъемлющую правовую базу, гарантирующую соразмерность соответствующих технологий и систем для конкретного случая использования» (то же самое). По мнению EDPS, некоторые приложения ИИ, такие как, например, распознавание лиц в реальном времени, «нарушают основные права и свободы до такой степени, что могут поставить под сомнение сущность этих прав и свобод» (там же, 7), подразумевая, что они могут быть вообще недопустимыми. EPDS сосредотачивает часть своего анализа на удаленной биометрической идентификации (RBI), которая может полагаться на ИИ или нет, и включает

живое выражение лица признание в общественных местах, но не ограничивается этим. Эти системы, как отмечает EDPS, «легко скрываются, не вызывают трения, часто представляются просто «экспериментом», но могут быть легко превращены во вездесущий и всеобъемлющий комплекс наблюдения» (там же, 20)[193].

Что касается прогнозирующей полицейской деятельности, EDPS заявляет, что она «может иметь негативные последствия, такие как чрезмерное использование полиции, как для коллективов, так и для отдельных лиц», и призывает в этом контексте разработать «инклюзивные модели управления, которые расширили бы возможности организаций, представляющих гражданское общество (например, НПО и другие некоммерческие ассоциации), чтобы они также могли помочь оценить влияние приложений ИИ на конкретные коллективы и общество в целом» (там же, 9). Что касается недискриминации, EDPS подчеркивает, что ИИ может иметь особые риски для «уязвимых групп», и выдвигает, что в отсутствие официально принятого юридического определения уязвимых групп должен применяться «контекстно-зависимый, прагматический подход» одобрено, чтобы охватывать «детей, пожилых людей и лиц с ограниченными возможностями, этнические меньшинства или исторически маргинализированные группы, женщин, сообщества LGBTQIA +, рабочих и других лиц, находящихся под угрозой исключения» (там же, 21). Наконец, в своей реакции на «Белую книгу» EDPS также отметила, что некоторые связанные с ИИ меры, выдвинутые в контексте борьбы с пандемией, сами по себе представляют собой или создают своего рода «ползучесть функций», которые могут иметь «сдерживающий эффект» в демократических обществах» (там же, 20).

Что касается закона о защите данных ЕС, сообщение Европейской комиссии отмечает двухлетие о применении GDPR повторил продолжающиеся двусторонние диалоги между ЕС и государствами - членами в целях обеспечения надлежащего осуществления на GDPR (COM (2020) 264 заключительный, 14). В Сообщении, в частности, признается, что частные компании, работающие на европейском рынке, могут быть привлечены к обмену данными в правоохранительных целях «на основании законного запроса», и что такие запросы могут привести к возникновению коллизий закона или возникновению противоречий с основными правами ЕС[194].

---

[193] Значимость проблем, связанных с RBI, не исключает, EDPS содержит нюансы, что аналогичные технологии, не нацеленные на идентификацию людей, также могут вызывать серьезные опасения: это может иметь место, например, в случае так называемого «обнаружения» в реальном времени эмоции (EDPS, Мнение 4/2020, 20).

[194] Европейская комиссия объявила в этом контексте, что «для улучшения таких переводов Комиссия привержена разработке соответствующих правовых рамок со своими международными партнерами, чтобы избежать коллизий права и поддерживать эффективные формы сотрудничества, в частности, путем предоставления необходимых данных меры защиты и тем самым способствовать более эффективной борьбе с преступностью» (COM (2020) 264 final, 13). Это, в частности, выражается в обязательстве «оценить, как можно

В апреле 2020 года Европейская комиссия обнародовала создание Экспертной группы по искусственному интеллекту в сфере внутренних дел для оказания помощи Генеральному директору Европейской комиссии по миграции и внутренних дел при подготовке законодательных предложений или политических инициатив, касающихся ИИ в сфере внутренних дел; наладить сотрудничество и координацию между Комиссией и государствами-членами или заинтересованными сторонами по вопросам, касающимся реализации законодательства, программ и политики ЕС в области ИИ в сфере внутренних дел; и обеспечить обмен опытом и передовой практикой в области ИИ в сфере внутренних дел. В его состав войдут представители властей государств-членов и ассоциированных стран Шенгенской зоны[195].

5.3. Европейский парламент

Европейский парламент рассматривал ИИ в различных политических контекстах - например, в феврале 2020 года он принял Резолюцию об автоматизированных процессах принятия решений: обеспечение защиты потребителей и свободное перемещение товаров и услуг (P9_TA (2020) 0032)[196].

В 2017 году Европейский парламент принял Резолюцию о последствиях больших данных для основных прав (конфиденциальности, защиты данных, недискриминации, безопасности и правоприменения), в которой содержится призыв к Европейской комиссии, EDPB и другим DPA издать руководящие принципы, рекомендации и передовой опыт для дальнейшего определения критериев и условий для решений, основанных на профилировании и использовании больших данных в правоохранительных целях» (EP, P8 TA (2017) 0076, параграф 25). В Резолюции подчеркивается, что «доверие граждан к цифровым услугам может быть серьезно подорвано государственной деятельностью по массовому наблюдению и неправомочным доступом правоохранительных органов к коммерческим и другим личным данным» (там же, параграф 27), и говорится, что «законодательство разрешает получение

облегчить сотрудничество между частными операторами и правоохранительными органами, в том числе путем переговоров двусторонние и многосторонние рамки для передачи данных в контексте доступа иностранных уголовных правоохранительных органов к электронным доказательствам» (там же, 18).

[195] Группа экспертов Комиссии по искусственному интеллекту в сфере внутренних дел (исх. № E03727 в Реестре экспертных групп Комиссии и других аналогичных организаций).

[196] Его пункт 10 включает в себя ссылку на адвокатуры: (ЕП) «подчеркивает, что в то время как автоматизированные процессы принятия решений могут повысить эффективность и точность обслуживания, люди должны всегда быть
в конечном счете, ответственности и возможности отменять решения, которые принимаются в контексте профессиональных услуг, таких как медицинские, юридические и бухгалтерские профессии, а также для банковского сектора; напоминает о важности надзора или независимого надзора со стороны квалифицированных специалистов
в случаях автоматизированного принятия решений, когда на карту поставлены законные общественные интересы»

государственными органами доступа к содержимому электронных сообщений на общей основе должно рассматриваться как компрометирующее сущность права на неприкосновенность частной жизни, как это установлено статьей 7 Хартии ЕС (там же, параграф 28)[197].

Европейский парламент также стал свидетелем ряда конкретных инициатив, связанных с ИИ. Создание бюджета для Обсерватории по искусственному интеллекту было запрошено, но отклонено Комитетом по бюджету Европейского парламента, что впоследствии привело к опасениям относительно возможного продолжения такой инициативы в виде рабочей группы (EP, P9 TA-PROV (2020) 0084, параграф 27).

Текущая работа над проектом отчета об искусственном интеллекте в уголовном праве и его использовании полицией и судебными органами в уголовных делах (LIBE, 2020/2016 (INI)) уже упоминалась. В документе, в частности, содержится призыв к мораторию на развертывание системы распознавания лиц для правоохранительных органов, а также набор рекомендаций, включая установление обязательной оценки воздействия на основные права и создание четкого и справедливого правового режима для возложения юридической ответственности за потенциальные неблагоприятные последствия, порождаемые передовыми цифровыми технологиями в поле.

18 июня 2020 года Европейский парламент принял решение создать специальный комитет по искусственному интеллекту в цифровую эпоху. Комитет должен начать свою деятельность после летних каникул.

5.4. Роль этики

Смягчение или стирание границ между законом и этикой, описанное в отношении Руководящих принципов этики ИИ HLEG, не является исключительным делом усилий Группы, а скорее является более распространенной тенденцией в европейских дискуссиях о цифровом регулировании. В этом контексте определенный тип «этики после соблюдения требований», открывающий пространство, характеризуемый как потенциально «неограниченное», был особенно заметен в дебатах на уровне ЕС в последние годы (Floridi, 2018). Пересечения между данными, этикой, искусственным интеллектом и политикой ЕС сложны и не помогают систематически составить последовательную картину того, что может быть роль этики в этой области, в

[197] Резолюция также отразила тот факт, что «разведывательные службы третьих стран и государств-членов все больше полагаются на обработку и аналитику таких наборов данных [больших данных], которые либо не подпадают под действие каких-либо правовых рамок, либо, в последнее время, были предмет законодательства, совместимость которого с первичным и вторичным законодательством Союза вызывает озабоченность и еще не установлена» (EP, P8_TA (2017) 0076, параграф D).

частности, в отношении (безусловно иной, возможно, дополнительной) роли права[198].

Работа над ИИ и этикой во всем мире чрезвычайно обширна и является результатом многолетних «интенсивных усилий» «разнообразного круга заинтересованных сторон», включая государственные органы и частные компании (Jobin, lenca & Vayena, 2019). С точки зрения содержания, хотя в соответствующих документах обычно используется совпадающая терминология - относящаяся, например, к прозрачности, справедливости и честности, ответственности, свободе и автономии, доверию, достоинству, устойчивости или солидарности — это не обязательно означает, что существует консенсус по поводу значение этих понятий или их значение (то же самое). AlgorithmWatch запустил глобальную инвентаризацию руководств по этике ИИ для компиляции структур и руководств, которые стремятся изложить принципы того, как системы для автоматизированного принятия решений могут разрабатываться и внедряться «этично», и в нем собрано более 160 руководств[199].

Этика уже играла значительную роль в глобальных дискуссиях вокруг больших данных несколько лет назад, особенно в связи с исследованиями[200]. Обсуждения ИИ и этики возникли во всех областях[201]. Еще одна целая ветка литературы касается возможности включения требований этики при разработке систем искусственного интеллекта[202]. По мнению некоторых авторов, акцент на

---

[198] Согласно руководству 2019 года, опубликованному Институтом Алана Тьюринга 1, этика ИИ - это набор ценностей, принципов и методов, в которых используются широко признанные стандарты правильного и неправильного, чтобы руководствоваться моральным поведением при разработке и использовании всех технологий». (Лесли, 2019, 3). Основная связь между этикой ИИ и законом будет заключаться в том, что моральный словарь этики ИИ опирается на рассуждение о правах человека, который, в свою очередь, «черпает вдохновение из Декларации прав человека ООН » (там же, 8). В руководстве содержится призыв, чтобы такое развитие сопровождалось «этической платформой», требующей набора действенных принципов, называемых FAST. Принципы отслеживания, состоящие из четырех понятий: справедливость, подотчетность, устойчивость и прозрачность (там же, 7).

[199] Как объяснили два участника команды, работающей над таким инвентаризацией, «этика ИИ», обнаруженная в этой базе данных, «часто находится между инструментально-экономической и этической точки зрения. Этика ИИ в этом смысле скорее является деловой этикой» (Giebler & Haas, 2020).

[200] Это особенно имело место после так называемого «скандала о заражении эмоциями в Facebook» в 2013 г., касающегося алгоритмической манипулирование эмоциями пользователей Facebook в исследовательских целях.

В то время американских ученых особенно интересовал тот факт, что исследование не было предметом стандартных процедур исследовательской этики, потому что оно финансировалось не государством, а корпоративным исследованием, которое в США имеет серьезные юридические последствия с точки зрения исследовательской этики. Таким образом, в частности, прозвучали призывы к сближению исследовательской этики и корпоративной этики, особенно в отношении данных и практики больших данных (boyd, 2016).

[201] В феврале 2020 года, например, Министерство обороны США приняло пять принципов «этического развития» возможностей искусственного интеллекта (Министерство обороны США, 2020). В качестве другого примера, в 2019 году министерство вооруженных сил Франции опубликовало отчет Целевой группы по ИИ, в котором содержится призыв к созданию министерского комитета, в частности, но не исключительно, по этическим вопросам, которые могут возникнуть при применении ИИ в военной сфере (AI Целевая группа, 2019 г.).

[202] Это связано с вопросом о том, можно ли каким-то образом операционализировать в математических или вычислительных терминах «этические требования»; аргументируя, например, что проектирование систем ИИ, а

этике как на главной призме, через которую следует учитывать риски, может составлять лишь «фазу», предшествующую другой фазе регулирования (Lapinski, 2018). В любом случае существует скептицизм по поводу добавленной стоимости «перехода к этическим принципам» с точки зрения измеримых эффектов, а также потому, что им часто не хватает механизмов обеспечения соблюдения (ИИ Now Institute, 2018, 9). Было заявлено, что частое использование слова «этика» в связи с алгоритмами может быть «индикатором тактического шага некоторых субъектов, которые хотят избежать строгого регулирования, указывая на неформальные нормативные концепции» (MSI-NET, 201 8, 42)[203]. Некоторые инициативы явно отличаются от подходов, ориентированных на этику, например, открыто признавая правозащитные аспекты в качестве первоочередной задачи[204].

В ряде европейских национальных стратегий искусственного интеллекта особое внимание уделяется этическим вопросам (Ван Рой, 2020; относительно Кипра, 20; Чехия, 24; Финляндия, 35; Франция, 36; Германия, 42). В Дании правительство подчеркнуло необходимость разработки и использования ИИ «в рамках соответствующего законодательства и с уважением прав граждан», что, в частности, потребует, чтобы «предприятия и государственные органы уделяли особое внимание этике данных» (Министерство финансов и Министерство промышленности, бизнеса и финансов правительства Дании, 2019, 8). В Бельгии, ИИ 4 Бельгия опубликовала доклад, отметив, что «важно, чтобы ввести этические принципы для поддержки разработки, внедрения и использования АТ» (ИИ 4 Бельгии Coalition, 2019, 14), и предложила «новая роль может быть создана для монитора соблюдение этих этических принципов: специалист по цифровой этике» (там же 15).

В 2018 году федеральное правительство Германии создало Комиссию по этике данных (Datenethikkommission) и поручило ей разработать этические ориентиры и руководящие принципы, а также конкретные рекомендации к действиям, направленные на защиту людей, сохранение социальной сплоченности, а также защиту и содействие процветанию в сфере информационной эпохе, чтобы конкретно ответить на ряд ключевых вопросов, сгруппированных вокруг принятия решений на основе алгоритмов (ADM), искусственного интеллекта и данных (Datenethikkommission, 2019, 13). Комиссия по этике данных открыто заявила, что, в частности, для вопросов,

---

также разработка требований справедливости в них, не является чисто математическим упражнением, а включает в себя ряд важных компромиссов, очень похожих на принятие человеческих решений в системе уголовного правосудия в целом: McNamara, et al. al, 2019,112.

[203] В некоторых случаях принятие этических норм в этом контексте открыто изображается как способ дальнейшего распространения ИИ, что должно быть одобрено теми, кто «предпочитает безопасность таким интересам,

как конфиденциальность» (McCarthy, 2019).

[204] Так обстоит дело, например, с Торонтской декларацией: защита права на равенство и недискриминацию в системах машинного обучения от мая 2018 года.

имеющих повышенное значение для основных прав, регулирование необходимо и не может быть заменено этическими принципами (там же, 15).

Во многих случаях в настоящее время существует по крайней мере некоторая степень двусмысленности, когда институты ЕС затрагивают роль закона и этики в отношении ИИ. В Союзе, который стремится к созданию большего количества документов фон дер Ляйена 2019 года, большое внимание уделялось важности «этических границ» и необходимости скоординированного «европейского подхода к человеческим и этическим последствиям искусственного интеллекта», а также призыв к принятию законодательства (Von der Leyen, 2019, 6). Также была ссылка на сохранение «этических стандартов», которые, похоже, связаны с GDPR, как будто, возможно, GDPR касается этических стандартов (то же самое).

Роль этики в этой области, как следует из вкладов Европейского парламента, неодинакова. В Резолюции Европейского парламента 2017 года о последствиях больших данных для основных прав он призвал правоохранительные органы «государств-членов» использовать аналитику данных для соблюдения высочайших этических стандартов при анализе данных», как способ содействия недопущению дискриминационная практика (P8_TA (201 7) 0076, пункт 32). Резолюция, принятая Европейским парламентом 12 февраля 2020 года об автоматических процессах принятия решений и защите потребителей, описывает «этические рекомендации, такие как принципы, принятые Группой экспертов высокого уровня Комиссии по искусственному интеллекту» как «отправную точку» (параграф D), чтобы двигаться к «общему подходу ЕС к развитию автоматизированных процессов принятия решений», который поможет обеспечить преимущества этих процессов и снизить риски во всем ЕС, избежать фрагментации внутреннего рынка и позволить ЕС лучше продвигать свой подход и его ценности во всем мире» (параграф E). EDPS, основной задачей которой является мониторинг соблюдения и предоставление рекомендаций по закону о защите данных, в последние годы уделял особое внимание «цифровой этике»[205]. Как-то в качестве контраргумента Совет обсудил возможность активного поощрения «развитие этики ИИ в отдельную дисциплину» (Совет I ЕС, 12224/19, 3).

[205] В отчете, опубликованном в 2018 году Консультативной группой по этике (EAG), перечислен ряд проблем, которые эта группа сочла актуальными для цифровой этики, среди которых упоминается «прогнозирующая полицейская деятельность». По наблюдениям ЕАГ, «прогнозирующая полицейская деятельность» «сопряжена с новым набором проблем», таких как ограниченная предсказуемость процессов принятия решений правоохранительными органами или риски предвзятости (EAG, 2018, 29). «Полиция может рисковать быть более заинтересованной в закономерностях, чем в сути, больше озабоченной прогнозом, чем наблюдаемыми фактами», - отмечает EAG (то же самое). Отчет был подготовлен «в ожидании» GDPR (там же, 7), но не упоминает LED и не делает каких-либо других конкретных ссылок на обработку данных в правоохранительных целях.

Двойственная связь между этикой и основными правами также проявляется на других форумах, включая Совет Европы. Европейская этическая хартия CEPEJ по использованию ИИ в судебных системах и их среде (CEPEJ, 2018) устанавливает в качестве первого принципа «Принцип уважения основных прав», описываемый как обеспечение «того, чтобы разработка и внедрение искусственного интеллекта инструменты и услуги совместимы с основными правами» (там же, 6). Руководящие принципы по искусственному интеллекту и защите данных, опубликованные в январе 2019 года Консультативным комитетом Совета Европы Комитет Конвенции о защите частных лиц в отношении автоматической обработки персональных данных (Конвенция 108) ссылается на «этические ценности» как на элемент «более широкого взгляда», который следует принимать при рассмотрении возможных результатов обработки данных. В этом смысле Руководящие принципы заявляют, что такой более широкий взгляд должен «учитывать не только права человека и основные свободы, но также функционирование демократий и социальные и этические ценности» (T-PD (2019) 01, 1).

В преамбуле Рекомендации Совета Европы о влиянии алгоритмических систем на права человека от апреля 2020 года указывается, что даже если «текущие инициативы государственного и частного секторов направлены на разработку этических руководящих принципов и стандартов для проектирования, разработки и постоянного развертывания алгоритмических систем» представляют собой «весьма долгожданное признание рисков, которые эти системы представляют для нормативных ценностей», эти инициативы, тем не менее, «не освобождают государства – члены Совета Европы от их обязательств в качестве основных хранителей» ЕКПЧ.

5.5. Поддержка ИИ, финансируемая ЕС

Большая часть поддержки ИИ и связанных с ним технологий ЕС осуществляется за счет финансирования. Фонды ЕС поддерживают ИИ, в том числе ИИ, связанный с правоохранительными органами, различными способами - некоторые из них открыто связаны с исследованиями в этой области, в то время как другие в основном не имеют исследовательского компонента. Инвестиции в ИИ были приоритетом для Европейской комиссии, которая удвоила свои инвестиции в ИИ в Horizon 2020 и выдвинула планы значительных инвестиций со стороны Horizon Europe и Программы цифровой Европы (COM (2019) 168 final, 1).[206]

[206] Президент Европейской комиссии заявила перед своим назначением, что она «позаботится о том, чтобы

Некоторые связанные с ИИ проекты, развернутые при поддержке финансирования ЕС, вызвали споры. Это, например, случай с проектом «умной полиции», запущенным в 2019 году полицией Греции в сотрудничество с телекоммуникационным оператором, включающее поставку «умных устройств» со встроенным программным обеспечением, обеспечивающим распознавание лиц и автоматическую идентификацию отпечатков пальцев, среди других функций, при поддержке Фонда внутренней безопасности (ISF) 2014-2020 Европейской комиссии (Chelioudakis, 2020). Другим примером является проект города Марселя под названием «Big Data de la tranquillite publique», запущенный в 2016 году для содействия сбору данных от институциональных партнеров с целью предотвращения определенных событий до того, как они произойдут, при софинансировании ЕС через Европейское региональное бюро. Схема Фонда развития (FEDER)[207] - события, которые в настоящее время находятся в центре местной борьбы против слежки, в частности, организованы НПО La Quadrature du Net (Meaker 2020).

Текущее финансирование исследований искусственного интеллекта в этой области отмечено двумя проблемами, которые могут иметь потенциально проблемные последствия для основных прав: во-первых, отсутствие четких конкретных рекомендаций, сопровождающих подачу и отбор предложений, и, во-вторых, серьезные ограничения в отношении прозрачности финансируемых исследований, включая, в первую очередь, информацию о соблюдении ими юридических и этических требований.

Что касается первого пункта, предложения по исследованиям обычно, помимо научной оценки, подаются на «Процедуру этической оценки»[208], оценивающую соответствие «этическим требованиям». Эти требования относятся к ряду вопросов, глобально укоренившихся в этике исследований, среди которых Европейская комиссия помещает защиту данных. Жест, который может привести к большему замешательству, чем ясности, «эксперты по этике», проводящие проверки для Европейской комиссии, могут принять решение во время введены соответствующие процедуры для включения в соглашение о гранте, которое должно быть подписано соответствующим консорциумом, ряда «этических требований», некоторые из которых могут относиться, например, к необходимости в соответствии с конкретными положениями GDPR, несмотря на это существо, как таковое, юридическое обязательство.

мы уделяли приоритетное внимание инвестициям в искусственный интеллект как через Многолетнюю финансовую структуру, так и за счет более широкого использования государственно-частных партнерств» (Von der Leyen, 2019, 13).

[207] См. страницу Le Big Data de la tranquillite publique.

[208] Это процедура, применяемая для проектов Horizon 2020, более подробная информация на соответствующей веб-странице.

Хотя некоторые из экспертов по этике могли быть наняты на основании их опыта в области защиты данных, не все из них обязательно обладают точными знаниями о законодательстве ЕС о защите данных, и в любом случае их систематически приглашают попытаться согласовать, если возможно, согласованное решение выбрать определенные заранее письменные заявления о «требованиях к защите данных». Формулировка этих требований, по-видимому, является наследием прошлых проверок и во многих случаях может не полностью применяться к рассматриваемому делу, поскольку фактическая Обязательства соответствующих контроллеров и обработчиков данных должны быть проанализированы с учетом применимых к ним конкретных национальных законов. В результате полезность всего упражнения сомнительна и часто может приводить к недоумению среди отобранных кандидатов, тем не менее, иногда им не остается ничего другого, кроме как попытаться выполнить наложенные «этические требования», вытекающие из этой процедуры, с целью получить требуемое финансирование.

Самый подробный совет, предоставляемый заявителям, имеет ряд недостатков. Руководство представлено в документе, представленном как «справочный документ» по «этике и защите данных» на соответствующем веб-сайте, но с оговоркой, согласно которой «он не является официальным руководством ЕС» (ЕС, 2018, 1). Документ настаивает на необходимости полагаться на согласие субъектов данных на обработку персональных данных о них[209], что на самом деле может быть не так. Другое заявление предупреждает, что «если в вашем предложении используются данные, обработанные или предоставленные органами, ответственными за предотвращение, расследование, выявление или преследование уголовных правонарушений, может также применяться Директива (ЕС) 2016/6801»: на самом деле это будет так, только если указанные органы в контексте исследовательского проекта осуществлять деятельность для упомянутых целей - при обработке данных для исследовательских целей применяется GDPR.[210]

В этом документе также говорится, что: «Если целью проекта является разработка технологий или методов наблюдения для правоохранительных целей, ваше предложение должно объяснять, почему наблюдение может считаться необходимым и соразмерным в демократическом обществе в соответствии с ценностями и принципами ЕС и законы» (ЕС, 2018). Однако этот вопрос вообще не упоминается в соответствующем «контрольном списке по вопросам этики», а также отсутствует в руководстве, предоставляемом

[209] В этом смысле: «Всякий раз, когда вы собираете персональные данные непосредственно от участников исследования, вы должны запрашивать их информированное согласие с помощью процедуры, которая соответствует минимальным стандартам GDPR» (ЕС, 2018, 10). Как широко известно и недавно было вновь подтверждено EDPB, GDPR предусматривает различные правовые основания, на которых может проводиться исследование (EDPB, Руководящие принципы 03/2020, 2020).

[210] См. Ст. 2 (1) LED.

заявителю для самооценки соблюдения этических требований (ЕС, Руководство программы Horizon 2020, 2019). Таким образом, неясно, как часто это может рассматриваться, если вообще.

Что касается прозрачности финансируемых исследований, следует отметить, что в целом предложения по исследованиям предусматривают публикацию одних результатов, в то время как для других планируется статус «конфиденциального» или «ограниченного ЕС». Часто бывает необходима конфиденциальность некоторых результатов, особенно в сфере безопасности. Однако Европейская комиссия в принципе имеет возможность требовать, чтобы некоторые мероприятия и результаты финансируемого проекта были открыты для общественного контроля. Европейская комиссия опубликовала руководство, подготовленное Генеральным директоратом по миграции и внутренним делам (DG HOME), в котором рекомендовалось классифицировать определенные типы исследований и результатов исследований в определенных конкретных областях, таких как, например, безопасность границ, в Horizon 2020. проекты (ЕС, Руководство по программе H2020, версия 2.2, 2020).

В таком руководстве не упоминается о необходимости классифицировать результаты с информацией о юридических и этических стандартах. Фактически также не рекомендуется классифицировать исследования в области «интеллектуальное наблюдение», определяемое как «использование распознавания образов и других методов искусственного интеллекта для анализа данных, полученных от более традиционных устройств безопасности, с целью выявления поведения, которое считается подозрительным или аномальным с учетом данного правового и социального контекста»[211].

Однако поражает то, что касается финансируемых ЕС исследований в области искусственного интеллекта и безопасности, так это отсутствие общедоступной информации о многих финансируемых проектах, в том числе об их соответствии правовым и этическим стандартам. В этом смысле NGO Privacy International утверждала, что «непонятно, каким образом некоторые из финансируемых проектов, которые поддерживаются, например, направленные на мониторинг потенциальных мигрантов в Европу, соответствуют правилам ЕС, в том числе по защите данных» (Privacy International, 2020a).

Особо прокомментированным случаем стал проект iBorderCtrl, финансируемый Horizon 2020, направленный на создание автоматизированной системы безопасности границ, включающей «автоматическое обнаружение обмана», несмотря на опасения по поводу научных и этических возможностей такого подхода. Также был прокомментирован тот факт, что, несмотря на

[211] Тем не менее, в документе отмечается, что, хотя «Классификация в этой области в настоящее время не предусмотрена», «он может измениться в будущем» (ЕС, Руководство по программе H2020, версия 2.2, 2020).

наличие опасений по поводу проекта, многие его результаты оставались скрытыми от общественного внимания (Leufer & Jansen, 2020). В мае 2020 года результаты финансируемых мероприятий, такие как материалы по «этике профилирования» и «риску стигматизации отдельных лиц» или «правовой и этический обзор в масштабах ЕС», будут описаны на веб-сайте проекта в том виде, в каком они представлены в Европейскую комиссию, но «конфиденциально» и, следовательно, недоступно для других исследователей или общественности[212].

Отсутствие прозрачности может резко повлиять на доверие населения к роли ЕС в поддержке ИИ в правоохранительной деятельности и уголовном правосудии.

Пример 1. Наблюдение за общественным пространством в реальном времени

Проект «Искусственный интеллект и компьютерное зрение для диагностики общественных пространств в реальном времени» был профинансирован в 2019 году (H2020-SMEInst-2018-2020-1), чтобы вывести на рынок решение для диагностики общественных пространств в реальном времени, в том числе Urban Security Eye линейка продуктов, нацеленная на обнаружение терроризма, подозрительного поведения и небезопасных зон (ЕС, 2019, 90). На веб-сайте координатора утверждается, что их продукты «настолько анонимны, что GDPR становится неактуальным», но, похоже, не предлагает каких-либо конкретных дополнительных разъяснений относительно правовых и этических последствий их работы.

Пример 2: автономные роботы на границе

Проект ROBORDER направлен на разработку полнофункциональных автономных систем наблюдения за границами с беспилотными мобильными роботами, включая решения для работы в воздухе, на воде, под водой и на земле, с мультимодальными датчиками. «Гетерогенная роботизированная система» должна быть повышена с возможностями обнаружения для раннего выявления преступной деятельности на границе и прибрежных районах. Все материалы, касающиеся вопросов этики, включая «Этический кодекс», по всей видимости, были расценены как полностью конфиденциальные и, следовательно, недоступные даже частично согласно веб-сайту проекта.

Пример 3: Предсказание и предотвращение преступлений.

Проект InterCONnected NEXt-Generation Immersive IoT Platform для обнаружения преступности и терроризма, прогнозирования, расследования и превентивных услуг (CONNEXIONS) описывает себя как решение,

[212] См. список результатов проекта здесь: https://www/iborderctrl.eu/Publications

охватывающее весь жизненный цикл правоохранительных операций, от «предупреждения и предотвращения преступлений до возникновения» до расследования «после происшествия». Он, в частности, связан с многоязычным автоматическим распознаванием речи онлайн-материалов, и его варианты использования охватывают угрозы на публичных мероприятиях, таких как футбольные матчи и фестивали. Согласно описанию в Службе общественной информации по исследованиям и разработкам (CORDIS), проект, запущенный в сентябре 2018 года, планировал «принять принципы этики и конфиденциальности путем разработки». В июле 2020 года публичные результаты не будут доступны в Интернете.

Пример 4: боты с интеллектуальными диалогами для раннего обнаружения террористов

TENSOR – это проект Horizon 2020, направленный на разработку платформы для помощи правоохранительным органам в раннем обнаружении террористической деятельности, радикализации и вербовки, как поясняется на веб-сайте проекта. Платформа описывалась как интегрирующая «набор автоматических и полуавтоматических инструментов», включая инструменты для мониторинга онлайн-контента, а также «проникновение в Интернет через интеллектуальных ботов с возможностью диалога». Весь профинансированный рабочий пакет финансируемого проекта был посвящен разработке «правовой и этической основы, которая будет лежать в основе» таких разработок; Пятерка участников проекта утверждала, что такая работа «гарантирует, что решения будут определяться законами о конфиденциальности и защите данных, которые защищают свободу граждан по всей Европе при использовании Интернета». Проект завершился в ноябре 2019 года. В июле 2020 года веб-сайт проекта объявил, как общедоступные в общей сложности четыре результата, ни один из которых не касается соответствующей правовой и этической основы, и ни один из них не является фактически загружаемым.

Реагирование на вспышку covid-19

Вспышка COVID-19 имела драматические последствия во всем мире, и ответные меры на кризис вызвали, по крайней мере потенциально, целый ряд последствий для основных прав человека. В этом разделе освещаются некоторые вопросы, которые кажутся особенно важными для размышлений о влиянии ИИ на основные права ЕС в области правоохранительной деятельности и уголовного правосудия. Раздел посвящен двум основным темам: во-первых, ответы на основе данных, которые имеют большое влияние на сбор и обработку – и, возможно, доступность – данных о лицах, и, во-

вторых, инициативы, предпринимаемые непосредственно правоохранительными органами.

Тем не менее, многие другие проблемы могут повлиять на развитие этой области. Среди них – усилия по ускорению цифровизации государственных услуг и, в первую очередь, отправления правосудия[213]. На работу правоохранительных органов также повлияло изменение значимости определенных видов преступлений (таких как, например, преступления, связанные с домашним насилием). По данным Интерпола, «киберпреступники извлекают выгоду из беспокойства, вызванного COVID-19, с помощью различных кибератак, таких как вредоносное ПО для сбора данных, программы-вымогатели, онлайн-мошенничество и фишинг» (Interpol, 2020).

Наблюдается общая тенденция к принятию или изменению целевого назначения технологических решений, преследующих несколько целей и опирающихся на быструю адаптацию частных компаний (Gershgorn, 2020). В целом, обработка данных и практика наблюдения увеличились во всем мире. В Китае программное обеспечение для распознавания лиц было адаптировано для обнаружения ношения масок уже в феврале (Jain, 2020)[214]; в Москве распознавание лиц использовалось для обеспечения соблюдения карантинных обязательств с марта (Habersetzer, 2020). В США компания Athena Security также в марте начала продавать «Систему выявления лихорадки на COVID-19», якобы выявляющую лихорадку «с помощью искусственного интеллекта», но без использования распознавания лиц как такового (Cox, 2020)[215]. В Сингапуре муниципальные власти решили протестировать четвероногого робота, продаваемого американской компанией по разработке робототехники в качестве инструмента, напоминающего посетителям парка о необходимости держаться на безопасном расстоянии друг от друга, в частности, путем трансляции предварительно записанных сообщений (Vincent, 2020).

Некоторые меры напрямую касались вопросов, связанных с автоматическим принятием решений. В апреле 2020 года организации

---

[213] Уже в начале апреля 2020 года, юстиции ЕС министры договорились активизировать усилия по обеспечению оцифровку своих судебных процедур, а также безопасный цифровой канал для всех процедур судебного сотрудничества (European Commission, 7 апреля 2020 года). Быстрый переход к онлайн-решениям создал проблемы
в некоторых государствах-членах; в Италии, например, ассоциация юристов по уголовным делам запросила участие итальянского DPA для оценки последствий принудительного переключения некоторых процедур уголовного правосудия на цифровые вопросы, в частности, с использованием Skype для бизнеса е Teams, оба из которых принадлежат Microsoft Corporation (Unione Camere Penali Italiane, 2020).

[214] Распознаванию лиц не обязательно мешает тот факт, что люди могут носить маски, поскольку поставщики технологий работали над тем, чтобы предлагать продукты, предназначенные для этого сценария (Yang, 2020).

[215] По сообщениям СМИ, Clearview AI в настоящее время будет предлагать государственным органам США решения по «отслеживанию контактов» с использованием изображений с камер наблюдения, с помощью которых он сможет собирать информацию о личности контактов людей (Thomsen, 2020; см. также Grind, McMillan & Mathews, 2020). Неясно, будет ли предлагаемая технология распознавания лиц в режиме реального времени для отслеживания контактов в ответ на пандемию COVID-19 (Markey, 2020).

гражданского общества США выразили обеспокоенность по поводу использования инструмента оценки рисков Pattern, изначально задуманного для присвоения баллов «общего рецидивизма», чтобы определить, какие лица, находящиеся в заключении, получат «приоритетное лечение» при принятии решений о переводе и освобождении в то контекст вспышки Covid-19 (Cook, 2020). Организации заявили, что шкалы риска алгоритмического рецидива не должны использоваться для оценки медицинского риска или играть какую-либо роль в определении того, кто получает доступ к адекватной медицинской помощи. Они также подчеркнули, что инструмент ранее оценивался как «способный увековечить расовое неравенство при принятии решений» и пострадал от «допущений, заложенных в его структуру закодированный на предвзятость по отношению к чернокожим, латиноамериканцам, беднякам, бездомным людям и людям с психическими заболеваниями» (там же, 2).

Возможность использования мобильных приложений («приложений») во многих пробудила творческий потенциал. «У нас были идеи для приложений от людей в возрасте 14-15 лет, от частных лиц, от небольших начинающих компаний, от огромных глобальных компаний», - заявил 25 марта 2020 года исполнительный директор Программы ВОЗ по чрезвычайным ситуациям в области здравоохранения, Майкл Райан, прежде чем добавить: «Это было самое выдающееся и самое удивительное проявление поддержки и сотрудничества, которое я видел в своей карьере» (ВОЗ, 2020, 1). В ответ на эпидемию было разработано несколько типов приложений, в том числе приложения для самооценки, приложения для сбора данных в исследовательских целях, приложения, связанные с понятием «сертификаты иммунитета», и приложения для «отслеживания контактов», а также приложения, сочетающие в себе различные из этих функций[216]. Развернутые приложения стали общедоступными вместе с различными мерами и подходами к управлению кризисом[217].

Системы, контролирующие температуру людей, получили распространение. Италия, например, приняла в марте 2020 года правила,

---

[216] В некоторых случаях доступными приложениями были уже существующие приложения, измененные в контексте эпидемии. В Колумбии НПО Fundacion Karisma проанализировала три местных приложения и обнаружила важный набор технических уязвимостей, а также серьезные пробелы с точки зрения прозрачности (Labarthe & Velasquez, 2020b). НПО указала, например, что самое популярное приложение было фактически построено на приложении, разработанном Бразилией для отслеживания в 2014 году других заболеваний, таких как лихорадка денге и зика, и запросила данные, не актуальные в текущей ситуации (Labarthe & Velasquez, 2020a).

[217] Южная Корея, например, внедрила модель «отслеживания и прослеживания», основанную на тестировании и строгой изоляции, а также на публичном разглашении личной жизни человека. Государственные органы действительно публично делились информацией о передвижениях людей, прошедших тестирование на заражение, предположительно, чтобы помочь другим оценить, могут ли они быть инфицированы. На практике это привело к проблемному раскрытию информации, а также к случаям шантажа (Kim, 2020a). В конце концов, сообщения средств массовой информации, связывающие серию заражений с гей-клубами, породили опасения по поводу негативной реакции против уже дискриминированного сообщества (Kim, 2020b).

предусматривающие измерение температуры в режиме реального времени для доступа к различным помещениям, как для рабочих, так и для других[218].

В то время как меры по обработке данных и надзору расширялись, некоторые гарантии основных прав оказались под давлением. В мае 2020 года правительство Венгрии приостановило применение ряда прав субъектов данных GDPR в рамках чрезвычайных мер в связи с коронавирусом и установило временные рамки для осуществления прав на средства правовой защиты, включая право подавать жалобу и право на эффективную судебную защиту, гарантированную GDPR. Представители гражданского общества связались с EDPB и призвали их обратиться к Европейской комиссии с просьбой начать процедуру нарушения прав Венгрии (Masse, 2020, 16)[219].

Вообще говоря, оценки событий, связанных с Covid-19, осторожны и делают упор на необходимости внимательно следить за ними. Некоторые предупреждали о возможном усилении «соблазна внедрить массовое наблюдение с использованием технологий для обеспечения безопасности общества» (Renda, 2020). В своей реакции на Белую книгу Европейской комиссии по ИИ, EDPS отметила, что некоторые связанные с ИИ меры, выдвинутые в контексте борьбы с пандемией, сами по себе представляют собой или создают своего рода «ползучую функцию», которая может иметь «сдерживающий эффект в демократических обществах» (EDPS, Мнение 4/2020, 20).

Ответы на основе данных

Важный аспект реакции ЕС на вспышку можно охарактеризовать как ориентированный на данные или как основанный на данных (Zanfir-Fortuna, 2020)[220]. Конкретно, на уровне ЕС обсуждались и поддерживались два основных типа мер, основанных на данных: использование данных о местоположении, предоставляемых поставщиками телекоммуникационных услуг государственным органам, и использование специальных приложений[221],

---

[218] См.: Protocollo condiviso di regolamentazione delle misure per il Contrasto e il contenimento della diffusione del virus Covid-19 negli ambienti di lavoro tra Governo e parti sociali del 14 marzo 2020, section 2.

[219] EDPB обсудила этот вопрос 8 мая 2020 г. (EDPB, 8 мая 2020 г.), но пришла к выводу, что необходимы дальнейшие объяснения, и, таким образом, обратилась к Венгерскому надзорному органу с просьбой предоставить дополнительную информацию о масштабах и продолжительности мер свое мнение о необходимости и соразмерности этих мер.

[220] Обзор основных документов, принятых учреждениями, агентствами и органами ФС по этим вопросам, можно найти в Законе о защите данных и обсерватории Covid-19 VUB/

[221] Китай изначально развернул систему, основанную на создании записи «событий близости» между людьми через мобильные приложения и отображении зеленого, желтого или красного кода с прямым указанием на ограничения передвижения (Ferretti et al., 2020, 5). Опираясь на такую инициативу, исследователи предложили основанную

в частности приложений, использующих «отслеживание контактов» с помощью Bluetooth.

24 марта 2020 года Европейская комиссия сообщила, что она изучила с операторами связи возможность сотрудничества в борьбе со вспышкой коронавируса. Тьерри Бретон, комиссар по внутреннему рынку, обсудил с руководителями европейских телекоммуникационных компаний и ассоциацией Глобальной системы мобильной связи (GSMA) возможности обмена метаданными геолокации для картирования и прогнозирования распространения вируса[222]. Государства приняли бы меры по отслеживанию местоположения в ответ на распространение коронавирусной болезни, в основном работая с телекоммуникационными компаниями для составления карты перемещений населения с использованием так называемых «анонимных» и агрегированных данных о местоположении (Dumbrava, 2020).

Голландское DPA категорически критически относится к самой возможности рассматривать как «анонимные» данные о местоположении. В этом смысле он опубликовал в апреле 2020 года документ об анонимности агрегированных данных о местоположении телекоммуникационных компаний, в котором был сделан вывод, что «без имитации сложно. Анонимизацию данных о местоположении практически невозможно отменить» (Autoriteit Persoonsgegevens, 2020). Объявляя о том, что EDPB опубликовал руководство по этому вопросу, голландский DPA вновь подчеркнул значение, которое он придает этому сообщению[223]. Что касается голландского DPA с несоответствующей, в частности связан с возможной заинтересованностью в каких - либо сохраненных данных полиции и службы безопасности (DutchNews, 2020).

8 апреля 2020 года Европейская комиссия опубликовала Рекомендацию об общем наборе инструментов Союза для использования технологий и данных для борьбы с кризисом COVID-19 и выхода из него, в частности, в отношении мобильных приложений и использования анонимных данных о мобильности (C (2020) 2296 final), в котором утверждалось, что «поэтому необходимо

на алгоритмах модель, которая позволила бы автоматизировать рекомендации по «стратифицированным по риску мерам карантина и физического дистанцирования», а также в конечном итоге усовершенствовать алгоритм, чтобы рекомендовать, например, карантин целых домохозяйств или районы (там же). Исследователи, выступающие за этот подход, выдвинули ряд возможных требований для получения доверия населения, среди которых можно назвать «использование прозрачного и проверяемого алгоритма» и «тщательный надзор и эффективные меры защиты при использовании данных» (там же).

[222] Подход Европейской комиссии к использованию данных электросвязи был описан как «в значительной степени основанный» на подходе, внедренном с середины марта бельгийской целевой группой «Данные против короны» (Mascini, 2020). Он полагается на операторов электросвязи предоставление данных о местонахождении пользователей мобильных телефонов с целью составления картины тенденций мобильности с использованием данных, которые считаются «анонимными».

[223] Путем ссылки на собственный документ в сноске.

разработать общий подход к использованию цифровых технологий и данных в ответ на текущий кризис» (там же, 1).

Что касается данных о местоположении, он пояснил, что «(с) некоторые компании, включая поставщиков телекоммуникационных услуг и основные технологические платформы, опубликовали или предоставили государственным органам анонимные и агрегированные данные о местоположении» (там же, 5). Что касается приложений, он отметил, что с начала кризиса COVID-19 было разработано множество мобильных приложений, «некоторые из них государственными органами» (там же, 3), и подчеркнул, что «отслеживание и отслеживание приложения полезны для государств-членов в целях отслеживания контактов и могут играть важную роль в сдерживании во время сценариев деэскалации» (там же, 4). Рекомендация уже намекала, что «в порядок обнаружения близости встречи между пользователями различных приложений для отслеживания контактов (сценарий, наиболее вероятный для людей, пересекающих национальные/региональные границы), следует предусмотреть возможность взаимодействия между приложениями» (там же, 5)[224].

По этим причинам Европейская комиссия объявила о создании «процесса разработки общего подхода, называемого набором инструментов, для использования цифровых средств решения кризиса» с упором на «пан-европейский подход к использованию мобильных приложений, координируются на уровне Союза» и «общая схема использования анонимизированных и агрегированные данные о мобильности населения» (там же, 7).

Использование приложений для отслеживания контактов иногда называют «цифровым» отслеживанием контактов, в отличие от «ручного» отслеживания контактов. Последний будет описывать практику повторного отслеживания с помощью людей контактов инфицированных лиц или лиц, которые, как предполагается, были потенциально инфицированы. Первый будет заключаться в автоматическом отслеживании «событий близости» между устройствами, которые могут рассматриваться как предполагающие контакт. Как так называемое «ручное», так и «цифровое» отслеживание контактов вызывает значительное вмешательство в фундаментальные права на

[224] В Рекомендациях указано: «Национальные органы здравоохранения, контролирующие цепочки передачи инфекции, должны иметь возможность обмениваться совместимой информацией о пользователях, у которых был положительный результат теста, с другими государствами-членами или регионами, чтобы решать проблемы трансграничных цепочек передачи» (C (2020) 2296 final). Высказывались опасения, что некоторые государства-члены могут потребовать от желающих войти на свою территорию использования определенного приложения или определенных типов приложений, и что может потребовать, чтобы по крайней мере близлежащие государства-члены предлагали соответствующие решения. Эти опасения, например, были высказаны на парламентских обсуждениях в Люксембурге (Chambre des Deputes du Grand-Duche de Luxembourg, 2020).

конфиденциальность и защиту данных несколькими способами[225]. «Ручное» отслеживание контактов в этом смысле обычно подразумевает, что инфицированный человек сталкивался с рядом особенно навязчивых вопросов о том, с кем он встречался за несколько дней до тестирования и какие контакты у него были, если таковые были.

С точки зрения основных прав ЕС, основное различие между так называемым «ручным» и «цифровым» отслеживанием контактов заключается в том, что первое из них основано на вмешательстве, которое в принципе имеет место только после того, как человек получил положительный результат теста, или проявляет симптомы или контактировал с кем-то, у кого был положительный результат теста или у кого есть симптомы - и, таким образом, затрагивает то, что в принципе можно рассматривать как меньшинство людей[226]. Отслеживание контактов через приложения, напротив, направлено на инициирование сбора данных о соответствующих контактах отдельных лиц заранее, с максимально широким охватом в качестве превентивного подхода, «на всякий случай» информация о таких контактах впоследствии будет полезна. С этой точки зрения, в принципе, чем больше людей будет заниматься сбором данных, тем лучше. Некоторые эксперты утверждали в этом смысле, что желательной целью с этой точки зрения было бы «приложение, которое использует каждый житель всех европейских государств-членов» (Mascini,2020).

Затем быстро последовали события в ЕС, в частности, с принятием 15 апреля 2020 года документа под названием Общий набор инструментов ЕС для государств-членов: мобильные приложения для поддержки отслеживания контактов в борьбе ЕС с COVID-19 Сетью электронного здравоохранения (сеть электронного здравоохранения, 15 апреля 2020)[227]. 16 апреля 2020 г. Европейская комиссия опубликовала Руководство по приложениям, поддерживающим борьбу с пандемией COVID 19, в отношении защиты данных (C/2020/2523).

---

[225] Кроме того, одно не исключает другого, и различие между ними может иногда стираться, например, когда государственные органы публично призывают население, включая здоровых людей, вести личные дневники всех людей, с которыми они сталкиваются. В EU DPA уже предоставили некоторые сведения о предлагаемых или развернутых приложениях, а также о «ручном» отслеживании контактов. Бельгийское агентство DPA в первом анализе законодательного предложения о создании базы данных для органов государственной власти в контексте борьбы с распространением COVID-19, в первую очередь, касалось отслеживания контактов вручную, но потенциально также может использоваться для приложений - включено отслеживание контактов, пришел к выводу, что предложение не удовлетворяет требованиям необходимости и соразмерности (DPA Бельгии, 29 апреля 2020 г.).

[226] В зависимости от степени распространения такое меньшинство может составлять большое количество лиц; все эти лица, тем не менее, будут соответствовать категории лиц, представляющих интерес по особой причине.

[227] Сеть электронного здравоохранения - это добровольная сеть, предоставляющая платформу для компетентных органов государств-членов, занимающихся цифровым здравоохранением: она была создана в соответствии
с Директивой 2011/24/EU, Директивой 2011/24/EU Европейского парламента и Европейского союза. Совет от 9 марта 2011 г. по применению прав пациентов в трансграничном здравоохранении, OJL 88, 4.4.2011, стр. 45-65.

В Резолюции, принятой 17 апреля 2020 года, Европейский парламент сослался на то, что на тот момент планировалось Европейской комиссией призвать провайдеров телекоммуникационных услуг передавать анонимные и агрегированные данные для ограничения распространения COVID-19, а также для «уже действующих национальных программ отслеживания и внедрения приложений, позволяющих властям отслеживать перемещения, контакты и данные о состоянии здоровья» (P9 TA(2020)0054, пункт 51). Европейский парламент подчеркнул важность обеспечения того, чтобы любые такие меры соответствовали закону ЕС о защите данных, и призвал Европейскую комиссию и государства-члены публиковать подробные сведения об этих схемах и обеспечивать их общественный контроль и полный надзор со стороны DPA (параграф 53). Что касается приложений для отслеживания контактов, он, в частности, потребовал, чтобы все хранилища данных были децентрализованы, а функционирование приложений было прозрачным, что позволяло проверять базовые протоколы и сам код (параграф 52).

13 мая 2020 года Сеть электронного здравоохранения опубликовала рекомендации по совместимости для утвержденных мобильных приложений для отслеживания контактов в ЕС (Сеть электронного здравоохранения, 13 мая 2020 года), предлагая рекомендации по трансграничной интероперабельности «утвержденных мобильных приложений для отслеживания контактов и связанных процедур» (там же, 3). В Руководстве также было объявлено, что Европейская комиссия должна создать «пространство вики (страница слияния)» также для взаимодействия с разработчиками приложений (там же, 10).

16 июня 2020 года Европейская комиссия объявила, что государства-члены «согласовали набор технических спецификаций для обеспечения безопасного обмена информацией между национальными приложениями для отслеживания контактов на основе децентрализованной архитектуры» (ЕС, 16 июня 2020 года). Объявление, по-видимому, относится к документу сети электронного здравоохранения, адресованному государствам-членам и Европейской комиссии с подробным описанием элементов взаимодействия (сеть электронного здравоохранения, 16 июня 2020 г.). Сеть электронного здравоохранения также опубликовала еще один документ о взаимодействии от 12 июня 2020 г. (и озаглавленный Спецификации взаимодействия для трансграничных цепочек передачи между утвержденными приложениями: основные элементы взаимодействия между решениями на основе COVID + решения, управляемые ключами) (Сеть электронного здравоохранения, 12 июня 2020 г.), в частности заявляет, что «чтобы уменьшить объем данных, загружаемых приложениями пользователя, приложения должны иметь возможность определять страны, в которых пользователь был в течение последних 14 дней» (там же, 6).

В июне 2020 года EDPB опубликовала Заявление о влиянии на защиту данных взаимодействия приложений для отслеживания контактов (EDPB, 16 июня 2020 года). В заявлении подчеркивается важность вопросов прозрачности, отмечая, что функциональная совместимость приводит к дополнительной обработке и раскрытию данных дополнительным объектам (там же, 2).

В июле 2020 года Европейская комиссия опубликовала обзор ситуации (ЕС, июль 2020 года), согласно которому подавляющее большинство государств-членов внедрили или планируют внедрить добровольные и временные мобильные приложения, которые поддерживают отслеживание контактов в рамках общественного здравоохранения стратегии борьбы с пандемией COVID-19 (там же, 4) - опираясь как на «децентрализованный», так и на «централизованный» подходы. Кроме того, было выявлено, что многие государства-члены внедрили или планируют внедрить другие мобильные приложения, такие как средства проверки симптомов (там же). Хотя некоторые государства-члены приняли специальное законодательство, касающееся таких приложений, некоторые отрицают необходимость такого конкретного законодательства (там же, 8). Что касается функциональной совместимости, в обзорном документе упоминаются планы Европейской комиссии по «настройке службы шлюза» для облегчения передачи данных между национальными приложениями для отслеживания контактов и серверами (там же 12).

По данным Европейской комиссии, государства-члены в настоящее время «работают над общим подходом к моделированию и прогнозированию развития пандемии COVID-19 с помощью анонимных и агрегированных данных о мобильности» (ЕС, июль 2020 г.).

Эти разработки имеют отношение к обсуждению ИИ в области правоохранительной деятельности и уголовного правосудия, прежде всего потому, что они приводят в действие новые методы обработки данных, потенциально охватывающие беспрецедентную доступность определенных типов данных, которые в конечном итоге могут быть доступны для целей правоохранительных органов.

6.2. Правоохранительные инициативы

Особенно заметное использование технологий правоохранительными органами во время пандемии коснулось дронов. В Италии, например, некоторые методы мониторинга с помощью дронов были разрешены в исключительных случаях, в частности, на том основании, что существует ограниченный риск причинения вреда людям, поскольку в общественных местах было меньше людей из-за мер изоляции (Dotta, 2020). То, как дроны

использовались для обеспечения соблюдения мер по ограничению передвижения, связанных с Covid-19, осуждалось гражданским обществом в некоторых государствах-членах, например, в Греции (Chelioudakis, 2020).

Во Франции 18 мая 2020 года Государственный совет опубликовал Решение о наблюдении с помощью дронов после действий двух организаций гражданского общества - La Quadrature du Net и La Ligue des Droits de l'Homme (Conseil d'Etat, 2020). В решении касались мер, позволяющих к изображениям захвата с помощью беспилотного летательного аппарата, с тем чтобы содействовать соблюдению строгой изоляции и социальное дистанцирование меры. Дроны, о которых идет речь, оснащены камерой и динамиком, позволяющими передавать сообщения общественности. По словам властей, ответственных за их использование, дроны не собирали никаких личных данных, в частности потому, что изображения отслеживались только в режиме реального времени, и группа лиц, наблюдающих за ними, не могла идентифицировать людей, за которыми наблюдали. Государственный совет, однако, заметил, что независимо от этой аргументации, факт заключался в том, что камеры дронов были оснащены зумом и что устройства могли летать достаточно низко, чтобы можно было получить подробное изображение людей, вынужденных рассматривать потенциально собранные данные как персональные данные (там же, пункт 16).

Политические рекомендации

Существует широкий консенсус в отношении того факта, что системы искусственного интеллекта в области правоохранительной деятельности и уголовного правосудия могут оказывать особенно серьезное влияние на основные права ЕС. В этой области системы искусственного интеллекта могут затронуть самую суть взаимоотношений между отдельными лицами и государственными органами, часто привлекая к участию частные компании, потенциально ускоряя потоки данных через юрисдикционные границы и ставя в ход множество новых вопросов о том, насколько важны решения принимаются, как их можно объяснить и как их можно обжаловать. Системы искусственного интеллекта в этой области могут влиять на основные меры безопасности, призванные гарантировать индивидуальную свободу и предотвратить злоупотребление властью. Таким образом, логично, что при обсуждении возможных сценариев возможного регулирования ИИ часто существует «общий консенсус» относительно необходимости определения хотя бы некоторых «четких красных линий для определенных сценариев

чрезвычайно высокого риска», которые могли бы оказать значительное влияние на людей и общество[228].

В своем политическом заявлении 2019 года Урсула фон дер Ляйен заявила, ссылаясь на планы по движению к «Европе, пригодной для цифровой эпохи», что «если мы увеличиваем инвестиции в прорывные исследования и прорывные инновации, мы должны принять эту неудачу. будет частью нашего пути» (Von der Leyen, 2019, 13). В 2017 году Европейская комиссия как-то аналогичным образом заявила, что «эксперименты являются важной частью исследования возникающих проблем в экономике данных» (COM (2017) 9 final, 17). Хотя эти подходы могут иметь некоторую ценность с экономической точки зрения в определенных контекстах, признание неудач и экспериментирование не могут быть наиболее подходящей формулой, когда на карту поставлены фундаментальные права.

Это исследование показало, что постепенное развертывание ИИ в сфере правоохранительной деятельности и уголовного правосудия, хотя и в некоторой степени находится в зачаточном состоянии, уже вызвало призывы к осторожности, а также случаи недоверия и сопротивления. Исследование также показало, что, хотя на уровне ЕС уже было предпринято много усилий, направленных на создание заслуживающей доверия экосистемы для появления ИИ, такие усилия еще не были полностью обоснованы подробным признанием специфики правовой базы в этом поле.

Принимая во внимание результаты исследования, приведенные ниже рекомендации, могут быть помещены вперед.

7.1. Полностью оценить актуальность и пробелы в существующей правовой базе

Как описано, многие дискуссии о возможной необходимости законодательного вмешательства в отношении ИИ основаны на интерпретации мер защиты данных, которые GDPR предоставляет отдельным лицам. В целом, но особенно в отношении обработки персональных данных в сфере правоприменения и уголовного правосудия, недостаточно ограничить соответствующую оценку чтением GDPR.

Крайне важно, во-первых, рассмотреть также правовые инструменты ЕС, такие как LED и EU-DPR. Но в равной степени необходимо выйти за рамки анализа правовых инструментов ЕС, в частности, к оценке национального

[228] Ссылка на такой общий консенсус на многостороннем семинаре по ИИ и распознаванию лиц, состоявшемся в Брюсселе в феврале 2020 года: Wiewiorowski, 2020.

законодательства, которое либо определяет GDPR, либо реализует LED, поскольку государства-члены могли принять исключения или отступления, которые изменяют гарантии, в конечном итоге доступные для физических лиц, когда данные о них обрабатываются в правоохранительных целях или в целях уголовного правосудия. Более того, в равной степени необходимо принимать во внимание обеспечение соблюдения соответствующих положений и опыт различных вовлеченных сторон[229]. Наконец, еще предстоит выяснить, любые возможные слабые места могут быть эффективно устранены способами, отличными от законодательного вмешательства, и, возможно, укрепление механизмов согласованности может быть достаточным решением[230].

7.2. Адаптировать инициативы к специфике области

Некоторые общие принципы, которые обычно считаются ключевыми для надежной экосистемы ИИ, могут столкнуться с конкретными проблемами в области правоохранительной деятельности и уголовного правосудия. Это, например, случай прозрачности. Таким образом, важно учитывать такие особенности с самого начала, а не разрабатывать общую основу для надежного ИИ, влияние которого в области правоохранительной деятельности и уголовного правосудия в конечном итоге будет сведено на нет или серьезно подорвано исключениями или отступлениями приняты во имя нужд правоохранительных органов или уголовного правосудия. Это может потребовать, например, обдумывания конкретных механизмов управления, которые были бы достаточно эффективными, чтобы компенсировать другие возможные ограничения прозрачности.

В Руководящих принципах Совета Европы по борьбе с воздействием алгоритмических систем на права человека прямо упоминается это противоречие, в частности, в связи с рекомендованными оценками воздействия на права человека[231]. В Руководящих принципах предлагается проводить «такие

---

[229] Может существовать значительный разрыв между определенными представлениями о предполагаемых сильных сторонах правовой базы защиты данных ЕС в свете появления ИИ, с одной стороны, и реальностью, которую воспринимают люди, чьи основные права находятся под угрозой. В этом смысле, например, хотя статья 22 GDPR должна предлагать значительные меры защиты от автоматического принятия решений (когда она применяется), последнее исследование Евробарометра по закону о защите данных показало, что большинство людей в ЕС никогда не слышали о своем праве высказывать свое мнение, когда они принимают автоматизированные решения (Kantar, 2019, 23). Необходимость большей ясности в толковании статьи 22 GDPR уже подчеркивалась многими (см., Например, Datenethikkommission, 2019, 28, 192).

[230] Тем не менее, такая оценка должна также учитывать, что согласованность, выходящая за рамки GDPR, менее формально разработана, но также и то, что даже в рамках GDPR механизмы согласованности кажутся не полностью эффективными в настоящий момент (см., например, отмечая недостаточную эффективность в отношении для определения согласованных критериев оценки защиты данных: Бельгийский орган по защите данных (DPA), 2020, 3.

[231] Рекомендация CM / Rec (2020) 1, Приложение, пункт B.5.3.

оценки воздействия как можно более открыто и с активным участием участие затронутых лиц и групп», а когда речь идет об алгоритмических системах высокого риска, «результаты текущих оценок воздействия на права человека, выявленные методы снижения рисков, а также соответствующие процессы мониторинга и анализа должны быть общедоступными без ущерба для соблюдения конфиденциальности в соответствии с законом»[232]. Более конкретно, «когда необходимо обеспечить соблюдение правил конфиденциальности, любая конфиденциальная информация должна быть представлена в отдельном приложении к отчету об оценке», которое должно быть доступно для соответствующих надзорных органов[233].

Также важно отметить, что любые возможные ограничения прозрачности в отношении субъектов данных делают еще более важным соблюдение других правовых принципов, таких как правовая определенность и предсказуемость[234].

7.3. Учитывайте необходимость специальных правил для определенных практик.

Многие проблемы, вызванные распознаванием лиц, и в первую очередь распознаванием лиц в общественных местах, требуют неотложного внимания и, возможно, конкретного ответа. Однако это не должно отвлекать внимание от возможной необходимости регулирования, выходящего за рамки такой конкретной практики. В этом смысле призывы к созданию нормативной базы для алгоритмического принятия решений в правоохранительных целях представляются весьма уместными в свете результатов этого исследования[235].

7.4. Разъяснить роль этики

Этические рамки и рекомендации могут быть полезны для создания надежной экосистемы для ИИ, но в настоящее время существует большая путаница в отношении того, какой должна быть связь между такими этическими рамками или рекомендациями и гарантиями основных прав. Такая путаница, если она будет продолжаться и дальше, может в конечном итоге

---

[232] То же.
[233] То же.
[234] Как указано в Своде (26) Регламента (ЕС) 2016/794 в отношении сотрудничества с правоохранительными органами, это область, в которой субъекты данных обычно не знают, когда их личные данные собираются и обрабатываются
и где используются личные данные, могут иметь очень значительное влияние на жизнь и свободы людей».
[235] В отношении Великобритании: Бабута, Освальд и Риник, 2018, vii.

нанести ущерб защите основных прав до такой степени, что может отвлечь внимание от необходимости соблюдения определенных юридических обязательств. В частности, этические рамки могут не обеспечивать необходимых гарантий доступа к средствам правовой защиты.

7.5. Укрепляйте доверие к финансируемым ЕС усилиям по ИИ

Было указано, что правительства должны быть «первыми», кто будет использовать ИИ таким образом, чтобы гарантировать и продвигать защиту данных и основные права в целом (Mantelero, 2019, 3); они должны придерживаться особо высоких стандартов, потому что они имеют прямое обязательство делать это, но также и потому, что государственная деятельность, как правило, должна служить примером для всего общества (Datenethikkommission, 2019, 212). Эти размышления могут быть расширены, чтобы охватить особую ответственность государственных органов, включая учреждения, агентства и органы ЕС, по поддержке исследований и решений в области ИИ за счет государственных средств.

Требования к прозрачности, надзору и подотчетности должны быть особенно высокими, когда средства ЕС используются для поддержки исследований ИИ, которые могут иметь серьезное влияние на основные права ЕС, например, исследования ИИ, связанные с безопасностью. Обзоры и оценки этических норм должны основываться на актуальных, соответствующих и соответствующих рекомендациях и сопровождаться четкими требованиями прозрачности, чтобы гарантировать, что финансируемое исследование надлежащим образом предлагает заслуживающие доверия решения и должным образом открыто для общественного контроля, особенно в части соблюдения правовых и «этических» стандартов.

Поскольку ожидается, что в ближайшие годы исследования в этой области будут приобретать все большее значение, предоставление конкретных рекомендаций по повышению доверия к исследованиям, финансируемым ЕС, имеет решающее значение, и, таким образом, необходим прогресс с точки зрения открытости. EDPS могла бы сыграть важную роль, усилив свою роль в обзоре определенных операций по обработке данных, финансируемых при поддержке фондов ЕС. EDPB может предоставить более качественное и подробное руководство, особенно для исследовательских работ, которые пересекают национальные границы[236].

[236] Также подчеркивая возможность конкретных рекомендаций по исследованиям, связанным с ИИ, в частности,

7.6. События в области скрининга, связанные со вспышкой Covid-19

В ответ на вспышку Covid-19 были приняты различные решения на основе данных и технологий, не обязательно немедленно сопровождаемые соответствующими техническими и правовыми гарантиями. Это потенциально может привести к ситуации повышенной уязвимости перед атаками кибербезопасности, включая угрозы, нацеленные на конфиденциальные данные. Это также может привести к ситуациям повышенной уязвимости из-за рисков неправильного использования власти. Даже если многие из одобренных инициатив не имеют явно правоохранительного измерения, они, тем не менее, позволяют обрабатывать данные, которые в конечном итоге могут быть доступны для правоохранительных целей, что создает особые риски для основных прав людей. Более того, из-за вспышки вируса и последующего управления кризисом основные права иногда серьезно ограничивались. Это обязывает проявлять особую бдительность, чтобы не допустить нанесения непоправимого ущерба ослабленным основным правам в результате кризиса, а также его ответных мер.

Ссылки

Access Now Europe, Европейская повестка дня в области прав человека в цифровую эпоху, ноябрь 2019 г.

Консультативный комитет по равным возможностям для женщин и мужчин, Заключение по искусственному интеллекту - возможности и проблемы для гендерного равенства, 18 марта 2020 г.

ИИ 4 Бельгия Коалиция, ИИ4 Бельгия Отчет, 2019.

Институт ИИ Now, Отчет ИИ Now 2018, декабрь 2018 г.

Целевая группа по ИИ, Искусственный интеллект в поддержку обороны, Ministere des Armees (Франция), сентябрь 2019.

Alfter, B., «Дания», M. Шпилькамп, «Общество автоматизации: учёт автоматизированного принятия решений в ЕС», AlgorithmWatch и BertelsmannStiftung, январь 2019 г., стр. 46-54.

Amnesty International, в ловушке матрицы: секретность, стигма и предвзятость в базе данных Met's Gangs Database, май 2018.

в трансграничных проектах: Datenethikkommission, 2019, 20.

Арройо, В. и Д. Леуфер (2020), «Распознавание лиц в процессе: определение эмоций и пола» в рассмотрение судебного дела в Бразилии», Access Now, 29 июня 2020 г.

Рабочая группа по статье 29, Руководство по оценке воздействия на защиту данных (DPIA) и определение является ли обработка «вероятно, приведет к высокому риску» для целей Регламента 2016/679, Принятого 4 апреля 2011 г. в последней редакции и Принятого 4 октября 2017 г., WP 248 rev.01.

- Руководство по автоматизированному индивидуальному принятию решений и профилированию для целей Регламента 2016/679, принятое 3 октября 2017 г., последнее пересмотренное и принятое 6 февраля 2018 г., WP251 ред. 01.

Ассоциация по вычислительной технике (ACM) Комитет по политике технологии США (USTPC), Заявление о принципах и предпосылках для развития, оценки и использования Несмещенных распознаваний лица технологий. 30 июня 2020.

Австрийская делегация в Совете, Примечание для Рабочей группы по обмену информацией и защите данных (DAPIX) о Prum следующего поколения (Prum.ng) - Отчеты фокус-групп / Отчет о распознавании лиц. 13356/19, Брюссель, 30 октября 2019 г.

Autoriteit Persoonsgegevens, об анонимности агрегированных данных о местоположении телекоммуникационных компаний, апрель 2020 г.

Бабута А. и М. Освальд, Аналитика данных и алгоритмы в полицейской деятельности в Англии и Уэльсе на пути к новым рамкам политики, периодический доклад, Королевский институт исследований в области обороны и безопасности при Соединенных Штатах Америки, февраль 2020 г.

Бабута, А., М. Освальд и К. Риник, Алгоритмы машинного обучения и правовые, этические и нормативные проблемы принятия полицейских решений. Отчет Уайтхолла 3-18, Королевский институт исследований в области обороны и безопасности при Соединенных Штатах, сентябрь 2018 г.

Барик, С., «Швеция разрешает полиции использовать технологию распознавания лиц». Медианама, 29 октября 2019.

Белфиоре, Р. «Защита личных данных, обрабатываемых в рамках сотрудничества полиции и судебных органов по уголовным делам», в: С. Руджери (ред.), Транснациональные расследования и защита основных прав в уголовном судопроизводстве, Springer, 2013 г., С. 355-370.

Бельгийских по защите данных, Оценка GDPR в соответствии со статьей 97 Вопросы к Совету по защите данных Authorities / Европейской защиты данных: Ответы от бельгийского надзорного органа, 2020.

- Objet: Demande d'avis concept un avant-projet d'aneTe Royal n ° XXX portant creation d'une banque de donnees aupres de Sciensano dans le cadre de la lutte contre la distribution of coronavirus COVID-19 (CO-A- 2020-042), Avis n ° 36/2020 от 29 апреля 2020 г.

Блатт. JJ. Некоторые наблюдения о системе распознавания лиц Clearview ИИ от того, кто ее действительно использовал, 6 мая 2020 г.

Боддингтон, П., на пути к этическому кодексу искусственного интеллекта, Springer, 2017.

Баучер П., почему важен искусственный интеллект (брифинг), Европейская парламентская исследовательская служба (EPRS), Отдел научного прогнозирования (STOA) PE 634.421, март 2019 г.

Boyd, d., «Исследование и практика: чему нас учит исследование «эмоционального заражения» Facebook». Этика исследований, 12 (1), 2016, стр. 4-13.

Brkan, M., «Правят ли миром алгоритмы? Принятие алгоритмических решений и защита данных в рамках GDPR и за его пределами», Международный журнал права и информационных технологий, 27: 2, 2019.

Брандейдж М. и др., Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий, февраль 2018 г.

Буоламвини, Дж. И Т. Гебру, «Гендерные оттенки: межсекторные различия в точности в коммерческой гендерной классификации». Конференция по справедливости, подотчетности и прозрачности, Proceedings of Machine Learning Research, 81, 2018.

Кэмпбелл. З. и К. Джонс. «Просочившиеся отчеты показывают, что полиция ЕС планирует создание общеевропейской сети баз данных распознавания лиц», The Intercept, 21 февраля 2020 г.

Каррера С. и М. Стефан, Доступ к электронным данным для целей уголовного расследования в ЕС, № 2020-01, Центр исследований европейской политики (CEPS), февраль 2020 г.

Кастро Д., М. Маклафлин и Э. Шивот, «Кто побеждает в гонке ИИ: Китай, ЕС или США?», Центр инноваций в области данных, 19 августа 2019 г.

Депутатская палата Великого герцога Люксембурга, Covid-19: vers un tracage numerioue? 28 апреля 2020.

Chelioudakis, E «Греция: пробуждение полиции, основанной на технологиях». Информация об Intel: European Voices on Surveillance, 29 июня 2020 г.

Комиссар Совета Европы по правам человека, Распаковка искусственного интеллекта: 10 шагов по защите прав человека - Рекомендация. Май 2019.

Комитет экспертов по Интернет-посредникам (MSI-NET), Исследование аспектов прав человека автоматизированных методов обработки данных (в частности, алгоритмов) и возможных регуляторных последствий, (докладчик: Бенджамин Вагнер), DGI (2017) 12 марта 2018 г.

Комитет экспертов по качественной журналистике в цифровую эпоху (MSI-JOQ), проект Рекомендации CM / Rec (20XX) XX Комитета министров государствам-членам о создании благоприятной среды для качественной журналистики в цифровую эпоху: 7-й проект от 26 сентября 2019 г., Совет Европы, MSI-JOQ (2018) 08rev6, 2019.

Комитет по гражданским свободам, правосудию и внутренним делам (LIBE) Европейского парламента, проект отчета об искусственном интеллекте в уголовном праве и его использовании полицией и судебными органами в уголовных делах. Докладчик: Тудор Чуходару, LIBE, 2020/2016 (INI), 8 июня 2020 г.

Conseil d'Ftat, Surveillance par drones (решение), 18 мая 2020 г.

Консультативный комитет Конвенции о защите частных лиц в отношении автоматической обработки персональных данных («Конвенция 108»), Практическое руководство по использованию персональных данных в полицейском секторе, Страсбург, 15 февраля 2018 г., T-PD (2018 г.) 01.

Кук, С., Письмо генеральному прокурору Барру об использовании оценки риска ШАБЛОНА при определении приоритетов выпуска в ответ на пандемию COVID-19, 3 апреля 2020 г.

Коуп, С. и Хусейн, С., «EFF в суд: пользователи социальных сетей имеют конфиденциальность и заинтересованы в свободе слова в своей публичной информации», Electronic Frontier Foundation (EFF), 30 июня 2020 г.

Coudert, F., «Европол Регулирование и цель Ограничение: Из «Силос подход, основанный на» в ... Что именно?», Европейский закон о защите данных (EDPL), Vol. 3, Number 3, 201 7, pp. 313-324.

Совет ЕС, Записка Комитета постоянных представителей (Часть 1) Совету по искусственному интеллекту - b) Заключения по согласованному плану по искусственному интеллекту (принятие), 6177/19, Брюссель, 11 февраля 2019 г.

- Записка Председателя Постоянного комитета по оперативному сотрудничеству по внутренней безопасности (COSI) о будущем направлении внутренней безопасности ЕС: новые технологии и внутренняя безопасность - Подготовка к дискуссии в Совете, 12224/19, COSI 184 ENFOPOL 400 CYBER 257 ЛИИ 949, Брюссель, 18 сентября 2019 г.

Кокс, Дж., Компания по видеонаблюдению заявляет, что развертывает камеры, обнаруживающие коронавирус, в США, Motherboard: Tech by The Vice, 17 марта 2020 г.,

Кокс, Дж. И Дж. Коблер, «Фирма слежения Banjo использовала секретную компанию и поддельные приложения для очистки социальных сетей». 9 марта 2020 г., Motherboard: Tech от The Vice.

Комиссия по этике данных Федерального правительства Германии (Datenethikkommission), Заключение (английская версия), Берлин, декабрь 2019 г.

DatИИnspektionen, DatИИnspektionen inleder tillsyn med anledning av Clearview ИИ, 6 марта 2020 г.

Datakalab, Politique de protection des donnees personnelles dans le cadre de la mise en oeuvre dispositif de détection de masques de protection respiratoire, апрель 2020

Дэвис, Б., М. Иннес и А. Доусон, Оценка использования полицией Южного Уэльса автоматизированного распознавания лиц, Научно-исследовательский институт полиции по вопросам преступности и безопасности, Институт Кардиффского университета, сентябрь 2018 г.

Де Брауэр, С., «Европейский парламент (снова) демонстрирует свою позицию в отношении искусственного интеллекта». Блог Access Now, 14 февраля 2020 г.

Де Капитани, Э., Жалоба и ходатайство о временном судебном запрете (Geulen & Klinger), 13 мая 2019 г.

Додд В., «MET удаляет сотни из матрицы банд после нарушения законов о данных». The Guardian, 15 февраля 2020 г.

Dotta G., «ENAC: autorizzati я Дрони за иль monitoraggio». Punto Informatico, 24 марта 2020 г.

Думбрава, С., «Отслеживание мобильных устройств для борьбы с коронавирусом». Блог Европейской парламентской исследовательской службы, 21 апреля 2020 г.

DutchNews: «Служба контроля конфиденциальности критикует план сопоставления телефонных данных с коронавирусом». DutchNews.nl, 3 июля 2020 г.

Сеть электронного здравоохранения, Общий набор инструментов ЕС для государств-членов: мобильные приложения для поддержки отслеживания контактов в борьбе ЕС с COVID-19 (версия 1.0). 15 апреля 2020.

- Руководство по совместимости для утвержденных мобильных приложений для отслеживания контактов в ЕС, 13 мая 2020 г.

- Спецификации взаимодействия для трансграничных цепочек передачи между утвержденными приложениями - Основные элементы взаимодействия между решениями на основе COVID + Keys, версия 1.0, 12 июня 2020 г.

- Странам-членам ЕС и Европейской комиссии по спецификациям совместимости для трансграничных цепочек передачи между утвержденными приложениями - Подробные элементы взаимодействия между решениями на основе COVID + Kevs. Версия 1.0, 16 июня 2020 г.

Консультативная группа по этике (EAG), На пути к цифровой этике. Европейский надзорный орган по защите данных (EDPS), 2018.

Европейская комиссия (ЕК), Политика Сообщества в отношении обработки данных: Сообщение Комиссии Совету, SEC (73) 4300 final, 21 ноября 1973 г.

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: На пути к процветающей экономике, основанной на данных, COM (2014) 442 final, 2 июля 2014 г.

- Стратегия единого цифрового рынка для Европы, COM (2015) 192 final, Брюссель, 6 мая 2015 г.

- Сообщение Комиссии Европейскому парламенту и Совету: более сильные и интеллектуальные информационные системы для границы и безопасности, COM (2016) 205 final, Брюссель, 6 апреля 2016 г.

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: построение европейской экономики данных, COM (201 7) 9 final, Брюссель, 10 января 2017 г.

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: Рабочая программа Комиссии на 2018 год: повестка дня для более объединенной, сильной и более демократичной Европы, COM (2017 г.) 650 финал, Страсбург, 24 октября 2017 г.

- Сообщение Комиссии Европейскому парламенту, Европейскому совету, Совету, Европейскому экономическому и социальному комитету и Комитету регионов по искусственному интеллекту для Европы, COM (2018) 237 final, Брюссель, 25 апреля 2018 г.

- Предложение о внесении поправок в Регламент Европейского парламента и Совета (ЕС) № 767/2008. Регламент (ЕС) № 810/2009. Регламент (ЕС) 2017/2226. Регламент (ЕС) 2016/399. Регламент XX / 2018 Регламент совместимости и Решение 2004/512 / ЕС и отменяющее Решение Совета 2008/633 / JHA. COM / 2018/302 final, Брюссель, 16 мая 2018 г.

- Сообщение Комиссии Европейскому парламенту. Совет. Европейский экономический и социальный комитет и Комитет регионов: Комиссия Рабочая программа 2019: Обеспечение того, что мы обещали, и готовиться к будущему, COM (2018) 800 окончательного, Страсбург, 23 октября 2018 года.

- Этика и защита данных, 14 ноября 2018 г. (ЕС, 2018).

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: согласованный план по искусственному интеллекту, Брюссель, COM (2018) 795 final, 7 декабря 2018 г.

- Руководство по программе Horizon 2020: как пройти самооценку по вопросам этики, Генеральный директорат по исследованиям и инновациям, версия 6.1, 4 февраля 2019 г.

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: укрепление доверия к человеко-ориентированному искусственному интеллекту. COM (2019) 168 final, Брюссель, 8 апреля 2019 г.

- Сообщение Комиссии Европейскому парламенту и Совету - Руководство по Положению о структуре для свободного потока неличных данных в Европейском Союзе, COM (2019) 250 final, Брюссель, 29 мая 2019 г.

- Сообщество пользователей в безопасности. Безопасные и устойчивые общества: картирование горизонта H2020 и финансируемые ЕС проекты по наращиванию потенциала в рамках программ на 2016-2018 годы, октябрь 2019 г.

- Руководство по программе H2020: Руководство по классификации информации в исследовательских проектах, Главное управление по миграции и внутренним делам, версия 2.2, 7 января 2020 г.

- Сообщение Комиссии Европейскому парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов: Рабочая программа Комиссии 2020: Союз, который стремится к большему. COM (2020) 37 final, Брюссель, 29 января 2020 г.

- Отчет Комиссии для Европейского парламента, Совета и Европейского экономического и социального комитета: Отчет о последствиях для безопасности и ответственности искусственного интеллекта, Интернета вещей и робототехники, COM (2020) 64 final, Брюссель, 19 февраля 2020.

- Белая книга по искусственному интеллекту - европейский подход к совершенству и доверию, COM (2020) 65 final, Брюссель, 19 февраля 2020 г.

- Сообщение в Европейский парламент, Совет, Европейский экономический и социальный комитет и Комитет регионов. Европейская стратегия обработки данных, COM (2020) 66 final, Брюссель, 19 февраля 2020 г.

- Сообщение в Европейский парламент в Совете. Европейский экономический и социальный комитет и Комитет регионов. Формируя цифровое будущее Европы, COM (2020) 67, финал, Брюссель, 19 февраля 2020 г.

- Ежедневные новости. 7 апреля 2020.

- Рекомендация Комиссии по общему набору инструментов Союза для использования технологий и данных для борьбы с кризисом COVID-19 и выхода из него, в частности, в отношении мобильных приложений и использования анонимных данных о мобильности, C (2020) 2296 final, Брюссель, 8 апреля 2020 г.

- Руководство по приложениям, поддерживающим борьбу с пандемией COVID 19, в отношении защиты данных, C/2020/2523, 16 апреля 2020 г.

- Ежедневные новости. 16 июня 2020.

- Сообщение в Европейский парламент и Совет. Защита данных как основа расширения прав и возможностей граждан и подход ЕС к цифровому переходу – два года применения Общего регламента защиты данных. COM (2020) 264 final, Брюссель, 24 июня 2020 г.

- Сообщение Комиссии Европейскому парламенту и Совету: дальнейшие шаги по приведению бывших достижений третьего столпа в соответствие с правилами защиты данных. Брюссель, COM (2020) 262 final, 24 июня 2020 г.

- Мобильные приложения для поддержки отслеживания контактов в битве ЕС против COVID-19: Отчет о ходе работы июнь 2020 г. июль 2020 г.

Европейская комиссия по эффективности правосудия (CEPEJ), Европейская этическая хартия использования искусственного интеллекта в судебных системах и их окружении, принятая CEPEJ на 31-м пленарном заседании (Страсбург, 3-4 декабря 2018 г.), CEPEJ (2018) 14.

Европейский совет по защите данных (EDPB): распознавание лиц в школе влечет за собой первый в Швеции штраф GDPR 22 августа 2019.

- Руководство 03/2020 по обработке данных о здоровье для целей научных исследований в контексте вспышки COVID-19, 21 апреля 2020 г.

- Проект повестки дня 26-го пленарного заседания, 8 мая 2020 г.

- Заявление о влиянии взаимодействия приложений для отслеживания контактов на защиту данных, принятое 16 июня 2020 г.

Европейский надзорный орган по защите данных (EDPS), Годовой отчет 2019.

- Мнение 4/2020 о Белой книге Европейской комиссии по искусственному интеллекту - европейский подход к совершенству и доверию, 29 июня 2020 г.

- Результат проведенного по собственной инициативе расследования использования учреждениями ЕС продуктов и услуг Microsoft, 2 июля 2020.

Европейская миграционная сеть (EMC), Годовой отчет о миграции и убежище за 2018 г., май 2019 г.

Европейский парламент (ЕП), Резолюция о программе наблюдения АНБ США, органы наблюдения в различные государства-члены и их влияние на основные права граждан ЕС и трансатлантические сотрудничество в юстиции и внутренних делах. (2013/2188 (INI)), 12 марта 2014 г.

- Резолюция о последствиях больших данных для основных прав: конфиденциальность, защита данных, недискриминация, безопасность и правоохранительные органы (2016/2225 (INI)), P8_TA (2017) 0076, 14 марта 2017 г.

- Постановление об автоматизированных процессах принятия решений: обеспечение защиты прав потребителей и свободного перемещения товаров и услуг. P9_ TA (2020) 0032, 12 февраля 2020 г.

- Резолюция о скоординированных действиях ЕС по борьбе с пандемией COVID-19 и ее последствиями, P9_TA (2020) 0054, 17 апреля 2020 года.

- Решение об исполнении общего бюджета Европейского Союза на 2018 финансовый год. Раздел I - Европейский парламент (2019 / 2056 (DEC)). P9_TA (2020) 0084, 13 мая 2020 г.

Агентство Европейского Союза по оперативному управлению крупномасштабными ИТ-системами в области свободы, безопасности и справедливости (eu-LISA), Тестирование границ будущего: Smart Borders Pilot: Вкратце о результатах, 2015 (2015a).

- Пилотный проект «Умные границы»: Приложения к Техническому отчету: Том 2. (2015b).

Агентство Европейского Союза по основным правам (EU FRA), Предотвращение незаконного профилирования сегодня и в будущем: руководство. Справочник, 2018 (2018a).

- #BigData: Дискриминация при принятии решений на основе данных, FRA Focus, 2018 (2018b).

- Технология распознавания лиц: соображения основных прав в контексте правоохранительной деятельности, FRA Focus, ноябрь 2019 г.

- Инициативы политики ИИ (2016-2020). Апрель 2020.

Комитет экспертов по аспектам автоматизированной обработки данных и различных форм искусственного интеллекта (MSI-AUT), ответственности и искусственного интеллекта (MSI-AUT): исследование последствий передовых цифровых технологий (включая системы искусственного интеллекта) для концепции ответственности в рамках прав человека (докладчик: Карен Йунг), DGI (2019) 05, Совет Европы, сентябрь 2019 г.

Ферретти Л. и др. «Количественная оценка передачи SARS-CoV-2 предполагает контроль над эпидемией с помощью цифрового отслеживания контактов». Наука, Vol. 368, Issue 6491, 8 мая 2020 г.

Борьба за будущее: «Реакция на обратную реакцию вынуждает Калифорнийский университет в Лос-Анджелесе отказаться от планов по слежке за распознаванием лиц в кампусе». Средний, 19 февраля 2020 г.

Флориди, Л., «Мягкая этика и управление цифровыми технологиями». Философия и технологии, Том 31, 2018, с. 1-8.

Fondazione Giacomo Brodolini (FGB), Обзор основных прав инструментов и программ сбора данных ЕС: Заключительный отчет, 2019.

Франко Аас, К., Вынесение приговоров в век информации: от Фауста до Macintosh, Routledge, Нью-Йорк, 2005.

Ф.Крстено, М., «Пилотная программа распознавания лиц в Германии разделяет публику», DW, 24 августа 2017.

Гарви, Си А. Бедойя и Дж. Фрэнки, «Бессрочный состав». Нерегулируемое полицейское распознавание лиц в Америке», Джорджтаунский юридический центр по вопросам конфиденциальности и технологий, 18 октября 2016 г.

Гейтс, К.А., Наше биометрическое будущее: технология распознавания лиц и культура наблюдения, New York University Press, 2011.

Генеральный секретариат Совета, записка для делегаций о выводах Совета относительно выполнения «решений Prum» через десять лет после их принятия, 11227/18, Брюссель, 18 июля 2018.

Гершгорн, Д. «Компании по распознаванию лиц рассматривают коронавирус как возможность для бизнеса». Один Ноль, 19 марта 2020 года.

Гиблер, С. и Л. Хаас, «Этика между деловым жаргоном и политикой: зачем беспокоиться?», Глобальная инвентаризация рекомендаций по этике ИИ, апрель 2020 г.

Гонсалес Фустер, Г., Отзыв на консультацию по Белой книге по искусственному интеллекту (ИИ), посвященной ИИ и гендерным вопросам: перспектива законодательства ЕС, 14 июня 2020 г.

Грейс, Дж., «Алгоритмические нарушения в полицейской деятельности Великобритании?», Журнал информационных прав, политики и практики, 03.01.2019.

Граф, Э., «Когда автоматизированное профилирование угрожает нашей свободе: неореспубликанская перспектива», Европейский закон о защите данных (EDPL), Vol. 3, номер 4, 2017, с. 441-451.

Гринд, К. Р. Макмиллан и А. В. Мэтьюз, для отслеживания вирусов. Правительства взвешивают инструменты слежки, которые расширяют границы конфиденциальности». Wall Street Journal, 17 марта 2020 г.

Хаберсетцер, Н., «Москва молча расширяет слежку за гражданами». Хьюман Райтс Вотч, 25 марта 2020.

Хамон, Р.,Х. Юнклевиц и И. Санчес, Надежность и объяснимость искусственного интеллекта: от технических к политическим решениям, Технический отчет JRC, Объединенный исследовательский центр (JRC), 30040 евро EN, 2020.

Харкорт, Б. Э., Против прогнозов: профилирование, контроль и наказание в актуарном возрасте, University of Chicago Press, 2008.

Хардинс, В.иА. Рамменс, «Предиктивная работа полиции как новый инструмент правоохранительных органов? Последние события и проблемы», Европейский журнал уголовной политики и исследований, 24 (3), 2017, стр. 201–218.

Хеннесси, М., «Объяснитель: что случилось с делом Грэма Дуайера о хранении данных в Верховном суде?», The Journal, 24 февраля 2020 г.

Группа экспертов высокого уровня по искусственному интеллекту (ИИ HLEG), Руководящие принципы этики для надежного искусственного интеллекта (ИИ). 8 апреля 2019 г. (2019a).

- Рекомендации по политике и инвестициям для надежного ИИ, 26 июня 2019 г. (2019b).

Группа высокого уровня по фейковым новостям и онлайн-дезинформации, Многоплановый подход к дезинформации, Европейская комиссия, март 2018 г.

Хилл, К., «Секретная компания, которая может положить конец конфиденциальности, какой мы ее знаем». The New York Times, 18 января 2020 г.

Офис комиссара по информации (ICO), Управление комиссара по информации Австралии и Управление комиссара по информации Великобритании открывают совместное расследование заявления Clearview ИИ Inc., 9 июля 2020 г.

Инновационный центр Международной организации уголовной полиции (Интерпол) и Межрегионального научно-исследовательского института ООН по вопросам преступности и правосудия (ЮНИКРИ), Искусственный интеллект и робототехника для правоохранительных органов, 2019 г.

Интерпол, Интерпол запускают информационную кампанию о киберугрозах COVID-19, 6 мая 2020 г.

IT-Pol, DPA Дании одобряет автоматическое распознавание лиц, Европейскую инициативу по цифровым правам (EDRi), 19 июня 2019 г.

Джайн Р., «ИИ для распознавания лиц ВИИdu поможет Китаю идентифицировать людей без масок». International Business Times, 17 февраля 2020 года.

Джелинек А., ответ EDPB депутатам Европарламента Софи ин'т Вельд, Морицу Корнеру, Михалу Симецке, Фабиене Келлер, Ян -Кристофу Этьен,

Анна Донат, Майте Пагазауртундуа, Оливье Шастель о приложении для распознавания лиц, разработанном Clearview ИИ, 10 июня 2020 г.

Джобин А., М. Ленка и Э. Вайена, «Глобальный ландшафт этических принципов ИИ». Nature Machine Intelligence, 2019, 1, стр. 389-399.

Юнкер, Дж. К., Новый старт для Европы: Mv-программа для рабочих мест. Рост. Справедливость и демократические перемены, Страсбург, 15 июля 2014 г.

Кантар, «Специальный Евробарометр 487a - март 2019 г.: Общие правила защиты данных», март 2019.

Кайзер-Брил, Н. «Неконтролируемое использование компьютерного зрения полицией сопряжено с высоким риском дискриминации». AlgorithmWatch, 28 апреля 2020 г.

Ким Н. «Страшнее коронавируса»: предупреждения о состоянии здоровья в Южной Корее раскрывают частную жизнь. The Guardian, 6 марта 2020 г.

«После сообщений СМИ о коронавирусе в Южной Корее возникли опасения по поводу ответной реакции на анти-aav». The Guardian, 8 мая 2020.

Koebler, J., E. МИИberg и J. Cox, 'Это небольшая компания Turning Юта B Паноптикуме Surveillance', материнские платы: Tech порок, 4 марта 2020 года.

Корфф, Д., Комментарии по избранным темам проекта Положения ЕС о защите данных, Лондон / Кембридж, 2012 г.

Лабарт, С. и А. Веласкес, CoronApp, Medellin me Cuida y CaliValle Corona al labratorio o como se hackea CoronAppsinsiquiera intentarlo-. 1 7 апреля 2020 г. (2020a).

Covid Apps в Колумбии Оценка цифровой безопасности и конфиденциальности Karisma. 28 апреля 2020 (2020b).

Лапинский, И., «Когда алгоритмы решают наши права». Фонд цифровой свободы, декабрь 2018 г.

La Quadrature du Net, La reconnИИssance faciale desmanifestant-e-sestdeia autorisee. 18 ноября 2019.

Ли Т.Б., «Шеф полиции Детройта добивается 96-процентного уровня ошибок при распознавании лиц». Ars Technica, 30 июня 2020.

Лесли Д., Понимание этики и безопасности искусственного интеллекта: руководство по ответственному проектированию и внедрению систем ИИ в государственном секторе, Институт Алана Тьюринга, 2019.

Лойфер и Янсен, «ЕС финансирует антиутопические проекты в области искусственного интеллекта». Евравтив, 22 января 2020.

Лайт, F «Россия строит одну из крупнейших в мире сетей распознавания лиц». The Moscow Times, 12 ноября 2019 года.

Линч, С., «Проблемы технологий распознавания лиц». Искусственный интеллект, ориентированный на человека - Стэнфордский университет, 23 апреля 2020 г.

Mac, R., C. Хэскинс и Л. Макдональд, «Признание лица App ClearView была Используется Министерства юстиции. ICE. Macv's. Walmart. И НБА». BuzzfeedNews, 27 февраля 2020 г.

Мантелеро А., Отчет об искусственном интеллекте – Искусственный интеллект и защита данных: проблемы и возможные средства правовой защиты. Консультативный комитет Конвенции о защите частных лиц в отношении автоматической обработки персональных данных (Конвенция 108), Страсбург, 25 января 2019 г., T- PD (2018) 09Rev.

Марки, EJ, Письмо сенатора Эдварда Дж. Марки Хоану Тон-Тату. Основатель и главный исполнительный директор ClearviewИИ, 30 апреля 2020 г.

Маскини, эксперт ЕС по европейскому реагированию на вирус: «Телекоммуникационные данные для отслеживания короны можно сделать анонимными», Innovation Origins, 11 апреля 2020 г.

Массе, Е. «Два года в соответствии с GDPR ЕС: отчет о ходе реализации», доступ сейчас, май 2020 г.

Управление полиции и преступности (MOPAC), Оценка воздействия на равенство. Матрица группового насилия. Версия 4. 2018.

Маккарти, О. Дж., «Искусственный интеллект и глобальное управление: переломить ситуацию с преступностью с помощью прогнозирующей полиции». Университет Организации Объединенных Наций, Центр политических исследований, 26 февраля 2019 г.

Макнамара, Дэниел и др., «Компромиссы в алгоритмической оценке риска: исследование случая домашнего насилия в Австралии» в книге Дейли А., М. Манн и С.К. Девитт, Good Data, Институт сетевых культур, Теория Спрос Vol. 29, 2019, с. 96-116.

Микер, М., «Борьба Марселя против слежки за ИИ». Coda, 26 марта 2020 г.

Министерство финансов и Министерство промышленности, бизнеса и финансов правительства Дании, Национальная стратегия искусственного интеллекта, март 2019 г.

Мольнар, П. и Л. Гилл, Боты у ворот: анализ прав человека в автоматизированном процессе принятия решений в канадской системе иммиграции и беженцев, Международная программа по правам человека (юридический факультет, Университет Торонто) и Citizen Lab (Munk Школа глобальных отношений и государственной политики Университета Торонто), 2018.

Монрой, М., «Решение PrQm: Европейские офисы уголовной полиции согласовали систему распознавания лиц». Архитектуры безопасности и сотрудничество полиции в ЕС, 11 марта 2020 г.

Мозур П., «Один месяц, 500 000 сканирований лиц: как Китай использует ИИ для профилирования меньшинства». New York Times, 14 апреля 2019 г.

Освальд, М., и Дж. Грейс, «Разведка, полицейская деятельность и использование алгоритмического анализа: свобода исследования, основанного на информации», Journal of Information Rights, Policy and Practice, 1.1, 2016.

Парламентская ассамблея Совета Европы, Рекомендация 2102 (2017) о технологической конвергенции. Искусственный интеллект и права человека, принята 28 апреля 2017 г.

Петерс, Б., «Распознавание лиц в аэропорту Брюсселя: лицом вниз в грязь». CITIPBIog, 17 марта 2020 г.

Пеннер. К., Общество автоматизации отчетов: Европа. 29 января 2019.

Перри, Л. У. и др., Предиктивная работа полиции: роль прогнозирования преступности в правоохранительных операциях, Rand Corporation, 2013.

Петерс, Дж., «IBM больше не будет предлагать, разрабатывать или исследовать технологию распознавания лиц». The Verge, 8 июня 2020 года.

Портер, Дж. «Facebook и LinkedIn стали последними, кто потребовал от Clearview прекратить очистку изображений для технологий распознавания лиц», The Verge, 6 февраля 2020 г.

Председательство в Совете, записка для Рабочей группы по обмену информацией и защите данных (DAPIX) по Prum следующего поколения (обрезка) - Планирование фокус-групп. 5556/19. Брюссель, 15 февраля 2019.

- Примечание для Рабочей группы по обмену информацией и защите данных (DAPIX) по мониторингу выполнения Директивы (ЕС) 2016/681 об

использовании данных записей имен пассажиров (PNR) - Состояние дел и дальнейшие шаги, 6300 / 19, Брюссель, 15 февраля 2019 г.

Privacy International, «МОНИТОРИНГ: Миллионы, потраченные ЕС на разработку технологии наблюдения, которая будет ЗА ВАС». 20 января 2020 г. (2020a).

- «Одна Рина, чтобы смотреть на всех». 25 января 2020 г. (2020b).

- Дело SvRI: знаковое решение для заявителей на получение льгот по всему миру». 24 февраля 2020 г. (2020c).

- Эта финансируемая правительством Великобритании программа искусственного интеллекта стремится сделать «распознавание лиц повсеместным» (Но конечно, мы, наверное, параноики насчет слежки за лицами). 3 марта 2020 года (2020d).

Ренда, А., «Will privacy be one of the victims of COVID-19?». Центр европейских политических исследований (CEPS), 23 марта 2020 г.

Reuters, «Германия: беженцы подают в суд на правительство за вторжение в частную жизнь». DW, 5 мая 2020 г.

Ричардсон, Р. Дж. Шульц и К. Кроуфорд, «Грязные данные. Плохие прогнозы: как нарушения гражданских прав влияют на данные полиции, системы прогнозирования и правосудие», 94 NYUL Rev. Online 192, февраль 2019, стр. 192-233.

Ричардсон Р., Дж.М. Шульц и В.М. Саутерленд, Отчет по судебным алгоритмам в США за 2019 г.: Новые вызовы государственному использованию систем алгоритмических решений, Институт ИИ Now, сентябрь 2019 г.

Робинсон Д., и Л. Кепке, «Застрял в шаблоне: первые данные о «прогнозируемой полицейской деятельности». Вверх 2016 г.

Ронсин Х. и В. Лампос, Углубленное исследование использования судебных систем искусственного интеллекта, в частности приложений искусственного интеллекта, обрабатывающих судебные решения и данные, Приложение I к Европейской этической хартии использования искусственного интеллекта в судебных системах и их окружении, принята CEPEJ на 31-м пленарном заседании (Страсбург, 3-4 декабря 2018 г.), CEPEJ (2018) 14, 2018.

Рубио И., «Las claves de la polémica por el uso de reconocimiento facial en los supermercados de Mercadona, El País, 7 июля 2020 г.

Sartor Г.Ф. Lagioia (2020), влияние OFTHE Общего регламента о защите данных (GDPR) по искусственному интеллекту. Европейская парламентская

исследовательская служба (EPRS), Отдел научного прогнозирования (STOA) PE 641.530 - июнь 2020 г.

Самойли С. и др., ИИ Watch - Определение искусственного интеллекта: к рабочему определению и таксономии искусственного интеллекта. Технические отчеты JRC, Европейский Союз, 2020.

Секретариат Совета I Европы, материалы для консультации по «Белой книге по искусственному интеллекту - европейский подход к совершенству и доверию», 19 января 2020 г.

Скотт М., «Европа ведет технический бой, связав одну руку за спиной». Политико, 24 февраля 2020.

Сингер Н. и М. Айзек, «Facebook заплатит 550 миллионов долларов за урегулирование иска по распознаванию лиц». New York Times, 29 января 2020 г.

Темме М., «Алгоритмы и прозрачность с учетом GDPR», Европейский закон о защите данных (EDPL), Vol. 3, Номер 4, 2017, с. 473-485.

Томсен. М. Федеральное правительство и три штата ведут переговоры со скандальной компанией по распознаванию лиц Clearview ИИ, чтобы отслеживать пациентов с коронавирусом и выяснять, с кем они контактировали, DИИly МИИl, 2 мая 2020 года.

TurB D., Европейский суд примет решение о массовой обработке данных о пассажирах, 22 января 2020 г.

Unione Camere Penali Italiane, Penale da Remoto e Protezione dei dati personali. L'Unione scrive al Garante. 14 апреля 2020.

Пресс-служба независимых экспертов по правам человека Организации Объединенных Наций (ООН), важное решение Нидерландов Суд пресекает попытки правительства шпионить за бедным - эксперт ООН. Пресс-релиз, 5 февраля 2020 г.

Специальный докладчик Организации Объединенных Наций (ООН) по вопросу о крайней бедности и правах человека, Доклад Специального докладчика по вопросу о крайней бедности и правах человека, A / 74/493, 2019.

Министерство обороны США (США), Резюме стратегии национальной обороны 2018 г.

Соединенные Штаты Америки: повышение конкурентоспособности американских военных, Вашингтон, округ Колумбия, 2018.

- Министерство обороны США принимает этические принципы искусственного интеллекта, пресс-релиз, 24 февраля 2020 г.

Министерство юстиции США (США), Прогностическая аналитика в правоохранительных органах: отчет Министерства юстиции, EPIC-16-06-15-DOJ-FOIA-20200319-Settlement-Production-pt1, ноябрь 2014 г.

Ваас Л., «Бостон запрещает государственное использование распознавания лиц». Naked Security от Sophos, 6 июля 2020 г.

Ван Бракель Р. (2019), «Бельгия», в М. Шпилькамп, «Общество автоматизации: учет автоматизированного принятия решений в ЕС», AlgorithmWatch и BertelsmannStiftung, январь 2019 г., стр. 39–44.

Ван Хобокен Дж. И др., Правовая основа распространения дезинформации через Интернет-сервисы и регулирование политической рекламы: Заключительный отчет, Институт информационного права (IViR), Амстердамский университет, 2019.

Ван Рой В., ИИ Watch - Национальные стратегии в области искусственного интеллекта: европейская перспектива в 2019 году. 30102 евро EN, Бюро публикаций Европейского союза, Люксембург, 2020.

Винсент J., Пятно робот напоминает parkgoers в Сингапуре, чтобы держать их расстоянии друг от друга, обочин, 8 мая 2020.

Фон дер Лейен У., «Союз, который стремится к большему: Mv повестка для Европы - Политические руководящие принципы для следующей Европейской комиссии на 2019–2024 годы», 2019.

Вагнер Дж. И А. Бенеке, «Национальное законодательство в рамках GDPR», Европейский закон о защите данных (EDPL), Vol. 2, Номер 3, 2016, стр. 353-361.

Вевиоровски В., 2020 г., «Признание лица и лица: проблемы и возможности», Блог Европейского надзорного органа по защите данных (EDPS), 21 февраля 2020 г.

Уилсон Д., «Алгоритмический патруль: будущее прогнозирующей полицейской деятельности», в А. Заврснике (ред.), Большие данные, преступность и социальный контроль, Routledge, Лондон и Нью-Йорк, 2017, стр. 108-127.

Всемирная комиссия по этике научных знаний и технологий (КОМЕСТ), Предварительное исследование этики искусственного интеллекта, ЮНЕСКО, 26 февраля 2019 г.

Всемирный экономический форум (ВЭФ), Схема ответственных ограничений на использование распознавания лиц: управление потоками, пилотный проект, Белая книга, февраль 2020 г.

Всемирная организация здравоохранения, виртуальная пресс-конференция по COVID-19 - 25 марта 2020 г., 2020 г.

Янг Ю., «Как Китай добился признания лиц в масках». Ars Technica, 18 марта 2020 г.

Юн Чи, Ф., «ЕС отказывается от идеи запрета распознавания лиц в общественных местах: бумага». Reuters, 30 января 2020.

Занфир-Фортуна, G «Политика Европейского Союза против пандемии на основе данных. Объяснил». Форум «Будущее конфиденциальности», 30 апреля 2020 г.,

Заврсник А., «Большие данные: что это такое и почему они важны для преступности и общественного контроля?» in A. Zavrsnik (ed.), Big Data, Crime and Social Control, Routledge, London and New York, 201 7, стр. 3-28. (2017a)

- Заврсник А., «Алгоритмический контроль преступности» в А. Заврснике (ред.), Большие данные, преступность и социальный контроль, Routledge, Лондон и Нью-Йорк, 2017, стр. 131-153 (2017b).

Приложение 1.

Сравнение алгоритмических прав на данные в GDPR и LED

В этом приложении содержится краткий обзор прав, предоставленных субъектам данных GDPR и LED в отношении профилирования и автоматического принятия решений. Эти права могут называться «алгоритмическими правами на данные» в той степени, в которой они непосредственно связаны с алгоритмической обработкой данных. Необходимо подчеркнуть, что это не означает, что другие права субъектов данных также могут не иметь значения. Также важно подчеркнуть, что эти права могут не применяться систематически, когда на карту поставлена обработка, связанная с правоохранительными органами и уголовным правосудием, поскольку как GDPR, так и LED допускают ограничения и отступления. Основная цель этого обзора - проиллюстрировать, что эти права, которые лежат в основе пересечения между законом ЕС о защите данных и искусственным интеллектом, получили различное содержание в GDPR и LED.

Представители DPA ЕС, собранные в качестве Рабочей группы по статье 29, разработали в 2017 г. Руководящие принципы по автоматизированному принятию индивидуальных решений и профилированию для целей Регламента

2016/679, которые позже были одобрены EDPB (A29WP, 2017/2018). Эквивалентных указаний относительно LED не существует. В Руководящих принципах в любом случае подчеркивается, что «профилирование и автоматизированное принятие решений могут создавать значительные риски для прав и свобод людей, которые требуют соответствующих гарантий» (там же, 5).

Выявленные риски связаны с непрозрачностью и дискриминацией. Непрозрачность может повлиять на сам факт профилирования и характер такого профилирования (то же самое). Обеспокоенность по поводу непрозрачности в основном решается в GDPR с помощью принципа прозрачности, который берет именно за отправную точку, что «процесс профилирования часто невидим для субъекта данных» (там же, 9). Кроме того, непрозрачность связана с тем фактом, что «люди имеют разные уровни понимания и могут столкнуться с трудностями в понимании сложных методов профилирования и автоматизированных процессов принятия решений» (то же самое). Проблемы дискриминации многочисленны: профилирование может закрепить существующие стереотипы и сегрегацию, привязать человека к определенной категории и ограничить его предлагаемыми предпочтениями. Кроме того, попадание в неправильную категорию может привести к неоправданной дискриминации (там же, 5).

Обеспокоенность по поводу дискриминации в основном рассматривается в GDPR с помощью принципа справедливости, который также присутствует в статье 4 (1)(a) Закона о защите данных. В Руководящих принципах подчеркивается, что «профилирование может быть несправедливым и создавать дискриминацию» (там же, 10). GDPR содержит ряд положений, направленных на обеспечение того, чтобы профилирование и автоматизированное принятие индивидуальных решений (независимо от того, включает ли оно профилирование) не использовались способами, которые оказывают неоправданное влияние на «права людей, в первую очередь, в дополнение к конкретным требованиям прозрачности и справедливости, обязательствам подотчетности; указанным правовым основаниям для обработки; правам отдельных лиц противодействовать профилированию и специально профилированию в маркетинговых целях; и, если при соблюдении определенных условий обязательство проводить оценку воздействия на защиту данных (там же, 6). Изложение (26) LED указывает: Принцип защиты данных справедливой обработки является отдельным понятием от права на справедливое судебное разбирательство как определено в статье 47 Хартии и в статье 6 Европейской конвенции о защите прав человека и основных свобод (ECHR)».

Согласно Руководству, «с учетом основного принципа прозрачности, лежащего в основе GDPR, контролеры должны четко и просто объяснять людям, как работает профилирование или автоматизированный процесс принятия решений» (там же, 16). «В частности», указывают они, «если обработка включает в себя принятие решений на основе профилирования (независимо от того, подпадают ли она под действие положений статьи 22), то тот факт, что обработка предназначена как для (a) профилирования, так и (b) принятие решения на основе созданного профиля должно быть четко разъяснено субъекту данных» (то же самое). В декларации (60) GDPR действительно говорится, что «субъект данных должен быть проинформирован о существовании профилирования и последствиях такого профилирования» в рамках принципа прозрачности GDPR (там же, 17).

Принцип прозрачности LED явно не упоминается как таковой. Это не фигурирует в статье 4, в которой перечислены Принципы, касающиеся обработки персональных данных: в статье 4 (1) (a) просто говорится, что «государства-члены должны обеспечить (...) обработку персональных данных законным и справедливым образом». Есть ссылка на прозрачность в выступлениях LED, в частности в Recital (26), в котором говорится, что «любая обработка личных данных должна быть законной, справедливой и прозрачной по отношению к заинтересованным физическим лицам и обрабатываться только для конкретные цели, изложенные в уставе». В LED нет явной ссылки на то, что субъект данных должен быть проинформирован о существовании профилирования и последствиях такого профилирования.

Помимо права на получение информации, существует право доступа, также упомянутое в статье 8 Хартии ЕС, вместе с правом на исправление. В Руководящих принципах говорится, что статья 15 GDPR о праве доступа «дает субъекту данных право получать подробную информацию о любых личных данных, используемых для профилирования, включая категории данных, используемых для создания профиля», и уточняет, что «(в дополнении к общей информацией об обработке, в соответствии со Статьей 15 (3), контролер обязан предоставить доступ к данным, используемым в качестве входных для создания профиля, а также доступ к информации о профиле и деталях, в каких сегментах был субъект данных помещен внутрь» (там же, 17).

Указанная статья 15 GDPR касается обязанности, налагаемой на контроллеры данных, «предоставлять копии обрабатываемых персональных данных». Право доступа в соответствии с индикатором не предусматривает эквивалентного обязательства, возложенного на контроллеры данных, по предоставлению копии данных, о которых идет речь. Подробное описание (43) LED указывает на то, что контроллеры данных могут соблюдать право доступа, предоставляя субъекту данных «полную сводку этих данных».

Субъекты данных имеют право на исправление и удаление. В Руководстве отмечается, что в GDPR «права на исправление и удаление применяются как к «входным личным данным» (персональные данные, использованные для создания профиля), так и к «выходным данным» (сам профиль или «ядро» закреплен за лицом)» (там же, 18). Право на исправление и стирание также присутствует в LED, хотя положение, устанавливающее их, также указывает, что в некоторых случаях отказ контроллера данных допустим. Государства-члены должны убедиться, что в таком случае контролер данных письменно уведомил субъекта данных об отказе, хотя государства-члены могут принять законодательные меры, ограничивающие, полностью или частично, обязательство предоставлять такую информацию при определенных условиях (Статья 16 (4) of the LED).

Субъекты данных имеют право возражать. В соответствии со статьей 21 GDPR право на возражение распространяется на случаи, когда обработка персональных данных «основана на пункте (e) или (f) статьи 6 (1), включая профилирование на основе этих положений», то есть, когда обработка «необходима для выполнения задачи, выполняемой в общественных интересах или для осуществления официальных полномочий, возложенных на контролера» (статья 6 (1) (e) GDPR) или обработка необходима для этих целей, законных интересов, преследуемых контролером или третьей стороной, за исключением случаев, когда такие интересы перекрываются интересами или основными правами и свободами субъекта данных, которые требуют защиты личных данных, в частности, если субъектом данных является ребенок) (статья 6 (1) (f) GDPR). Эквивалентного права на объект под LED нет.

Статья 22 GDPR, все еще находящаяся в главе GDPR о правах субъектов данных, называется Автоматизированное индивидуальное принятие решений, включая профилирование, и в ее первом параграфе говорится, что «Субъект данных имеет право не подвергаться решению, основанному исключительно на автоматизированная обработка, включая профилирование, которая порождает правовые последствия в отношении него или нее или аналогичным образом существенно влияет на него или ее». Руководящие принципы придерживаются той точки зрения, что использование термина «право» здесь не означает, что статья 22 (1) применяется только тогда, когда субъект данных активно ссылается на нее. Вместо этого статья 22 (1) GDPR установит общий запрет на принятие решений, основанных исключительно на автоматизированной обработке, тем не менее, применяемый в ограниченном числе обстоятельств (решение, основанное исключительно на автоматизированной обработке, и имеет юридические последствия или аналогично существенно влияет на кого-то), и возможны исключения. Согласно руководящим принципам, статья 22 GDPR предусматривает, что в соответствии с GDPR, как правило, существует общий запрет на полностью автоматизированное принятие индивидуальных

решений, включая профилирование, имеющее юридическую или аналогичную значимость эффект», хотя «есть исключения из правила», даже если «там, где применяется одно из этих исключений, должны быть приняты меры для защиты прав и свобод, и законных интересов субъекта данных» (там же, 19).

Статья 22 (1) GDPR применяется к решениям, основанным исключительно на автоматизированной обработке, включая профилирование, которые имеют правовые последствия в отношении субъекта данных или аналогичным образом существенно влияют на него. В Руководящих принципах разъясняется, что «обработка, которая может иметь незначительное влияние на отдельных людей, в целом может иметь значительное влияние на определенные группы общества, такие как группы меньшинств или уязвимые взрослые» (там же, 22).

Меры предосторожности, которые должны применяться при автоматизированном принятии решений, основанном исключительно на автоматизированной обработке, которая порождает правовые последствия или аналогичным образом существенно влияет на субъект данных, могут включать право на получение информации (в частности, на получение значимой информации о задействованной логике, а также значение и предполагаемые последствия для субъекта данных) и другие гарантии, такие как право на вмешательство человека и право оспаривать решение (рассматривается в статье 22 (3)) (там же, 20).

В индикаторе есть ссылка на государства-члены, которые должны установить, что решения, основанные исключительно на автоматизированной обработке, включая профилирование, которые имеют неблагоприятные правовые последствия в отношении субъекта данных или существенно влияют на них, должны быть запрещены, если это не разрешено ЕС или членом Закона штата, которому подчиняется контролер и который обеспечивает надлежащие гарантии прав и свобод субъекта данных, по крайней мере, право на вмешательство человека со стороны контролера (статья 11 (1) Закона об управлении данными). Таким образом, автоматизированные решения, приводящие к неблагоприятным юридическим последствиям, не полностью запрещены согласно Закону о законах, а обусловлены наличием положения закона, обеспечивающего некоторые гарантии. Статья 11 LED, в отличие от статьи 22 GDPR, появляется за пределами главы о правах субъектов данных. Нет явной ссылки на необходимость предвидеть право оспаривать решение, хотя есть упоминание об этом вопросе в Recital (38), который изображает возможность оспаривать решение как подходящую гарантию при оценке личных аспектов человека основана исключительно на автоматизированной обработке и имеет неблагоприятные правовые последствия или существенно влияет на них.

В отношении этих мер предосторожности в Руководстве отмечается, что «любая обработка, которая может привести к высокому риску для субъектов данных, требует от контролера проведения оценки воздействия на защиту данных (DPIA)», которая может быть «особенно полезной для контроллеров, которые не уверены, подпадает ли их предлагаемая деятельность под определение Статьи 22 (1), и, если это разрешено определенным исключением, какие меры защиты должны быть применены» (там же, 20). Как GDPR, так и LED предусматривают необходимость DPIA в некоторых случаях (см. Статью 35 GDPR и статью 27 LED). Однако требования к DPIA отличаются. GDPR, в частности, устанавливает, что «здесь уместно, контролер должен запрашивать мнение субъектов данных или их представителей о предполагаемой обработке» (статья 35 (9) GDPR), в то время как LED не имеет эквивалентного положения.

В соответствии с GDPR в исключительных случаях можно выполнить обработку, описанную в статье 22 (1), если решение (a) необходимо для выполнения или заключения договора, (b) разрешено законодательством ЕС или государства-члена, в отношении которого контролер должен устанавливать соответствующие меры для защиты прав и свобод и законных интересов субъекта данных; или (c) на основании явного согласия субъекта данных. Что касается пункта (b), в декларации (71) GDPR отмечается, что это может относиться к «целям мониторинга и предотвращения мошенничества и уклонения от уплаты налогов, осуществляемым в соответствии с положениями, стандартами и рекомендациями институтов Союза или национальных надзорных органов, а также для обеспечения безопасности и надежность услуги, предоставляемой контролером».

В соответствии со статьей 22 (4) GDPR, автоматизированное принятие решений, подпадающих под действие статьи 22 (1) GDPR, которая включает особые категории персональных данных, допускается только при следующих совокупных условиях, подпадающих под действие применимой статьи 22 (2) освобождение; и подпадающие под действие пункта (a) или (g) статьи 9 (2), которые относятся к необходимости явного согласия субъекта данных; или необходимость по причинам существенного общественного интереса на основании законодательства ЕС или государства-члена, которое должно быть соразмерным преследуемой цели, уважать сущность права на защиту данных и предусматривать подходящие и конкретные меры для защиты основных прав и интересов субъекта данных. В обоих случаях контролер должен принять соответствующие меры для защиты прав и свобод субъекта данных и законные интересы. В статье 11 LED нет ссылки на согласие. В соответствии с этим положением решения, подпадающие под действие статьи 11 LED, не должны основываться на особых категориях персональных данных, «если не приняты соответствующие меры для защиты прав и свобод, и законных интересов субъекта данных».

Переходя конкретно к правам субъекта данных, связанных с решениями, подпадающими под действие статьи 22 GDPR, в Руководстве отмечалось, что «с учетом потенциальных рисков и вмешательства, которые профилирование, выявленное статьей 22, представляет для прав субъектов данных, контролеры данных должны быть особенно помнить о своих обязательствах по обеспечению прозрачности» (там же, 24). Статьи 13 (2) (f) и 14 (2) (g) GDPR требуют, чтобы контроллеры данных предоставляли информацию о «существовании автоматизированного принятия решений, включая профилирование, о котором говорится в статье 22 (1) и (4) и, по крайней мере, в этих случаях значимая информация о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта данных».

Как пояснила Рабочая группа по статье 29, это означает, что в соответствии с GDPR контролеры данных должны информировать субъекта данных о том, что они участвуют в этом виде деятельности, предоставлять значимую информацию о задействованной логике и объяснять значимость и предполагаемые последствия обработки. Согласно Руководству, даже если автоматическое принятие решений и профилирование не подпадают под действие статьи 22 (1) GDPR, «тем не менее, предоставление вышеуказанной информации является хорошей практикой» (AWP29, 2017/2018, 25). Более того, он добавляет, что в любом случае контроллеры данных «должны предоставить субъекту данных достаточную информацию, чтобы сделать обработку справедливой» (то же самое, со ссылкой на Recital (60)).

Под LED нет эквивалентных информационных обязательств. Положение, детализирующее «Информация, которая должна быть предоставлена или предоставлена субъекту данных», то есть статья 13 LED, не включать любые ссылки на профилирование или автоматическое принятие решений. Единственным явным указанием на профилирование в Обзоре LED является намек на тот факт, что профилирование, которое приводит к дискриминации в отношении физических лиц на основе персональных данных, которые по своей природе являются особенно чувствительными в отношении основных прав и свобод, «должно быть запрещено в соответствии с условиями, изложенными в статьях 21 и 52 Хартии» (изложение (38) LED).

Что касается связи между решениями, подпадающими под действие статьи 22 GDPR, и правом доступа, статья 15 (1) (g) устанавливает, что субъекты данных, осуществляющие свое право доступа, имеют право получать информацию о «существовании автоматизированного решения - создание, включая профилирование, указанное в Статье 22 (1) и (4), и, по крайней мере, в этих случаях, значимую информацию о задействованной логике, а также о значении и предполагаемых последствиях такой обработки для субъекта

данных». Там нет ссылки на необходимость предоставить подробное объяснение, почему решение конкретно было принято.

В Руководстве со ссылкой на GDPR отмечается, что «при осуществлении своих прав, предусмотренных статьей 15, субъект данных может узнать о решении, принятом в отношении него или нее, в том числе о решении, основанном на профилировании» (там же, 27). В этом случае «контроллер должен предоставить субъекту данных с общей информацией (в частности, от факторов, принимаемых во внимание в процессе принятия решений, а также на их соответствующих «вес» на агрегированном уровне), который также является полезным для него или ее оспорить решение» (то же самое). Это относится к обязательствам по прозрачности и правам субъектов данных в законодательстве ЕС о защите данных: именно благодаря информированию об определенных методах обработки данных субъект данных сможет и в дальнейшем осуществлять свои права.

Что касается подходящих мер защиты, в Руководстве указано в отношении GDPR, что требование «вмешательства человека» связано с тем фактом, что «любая проверка должна проводиться лицом, имеющим соответствующие полномочия и возможности для изменения решения», и что рецензент должен предпринять тщательная оценка всех соответствующих данных, включая любую дополнительную информацию, предоставленную субъектом данных» (там же, 27).

Подходящие гарантии согласно GDPR включают, помимо права на вмешательство человека, право субъекта данных выражать свою точку зрения и право оспаривать решение. В Руководящих принципах указано, что контролер «должен предоставить субъекту данных простой способ реализации этих прав», и что они подчеркивают «необходимость прозрачности обработки», поскольку «субъект данных может только оспорить решение или выражают свою точку зрения, если полностью понимают, как это было сделано и на какой основе» (там же, 27).

Другие меры предосторожности, выделенные в Руководстве, включают меры предосторожности, направленные на снижение риска ошибок или предвзятости в собранных или совместно используемых данных или в автоматизированном процессе принятия решений, которые могут привести к «неправильным классификациям: и оценки, основанные на неточных прогнозах: на физических лиц» (там же, 27). Эти меры предосторожности могут включать в себя «частое проведение оценок наборов данных, которые они обрабатывают, для проверки на предмет предвзятости, и разработку способов устранения любых предвзятых элементов, включая любую чрезмерную зависимость от корреляций» или «систем, которые проверяют алгоритмы и регулярные проверки точности и актуальности автоматизированного принятия

решений, включая профилирование» (там же, 28). Кроме того, контролеры должны внедрить соответствующие процедуры и меры для предотвращения ошибок, неточностей или дискриминации на основе особых категорий данных, меры, которые следует использовать на циклической основе: не только на стадии проектирования, но также постоянно и обеспечивая результат такого тестирования учитывается при проектировании системы (то же самое). Все это связано с Декларацией (71) GDPR, в которой упоминается необходимость использования соответствующих математических или статистических процедур.

Это исследование, проведенное по заказу Департамента политики Европейского парламента по правам граждан и по запросу Комитета LIBE по конституционным вопросам изучается влияние искусственного интеллекта на основные права в области правоохранительной деятельности и уголовного правосудия с точки зрения Европейского союза. В нем представлена применимая правовая база (в частности, в отношении защиты данных), а также анализируются основные тенденции и ключевые обсуждения политики. В исследовании также рассматриваются события, произошедшие после вспышки Covid-19. В нем утверждается, что серьезность и масштаб проблем могут потребовать вмешательства на уровне ЕС, основанного на признании специфики региона.

IP / C / LI BE / IC / 2019-083
ISBN для печати 978-92-846-6938-7|doi: 10.2861/138135|QA-04-20-418-RU -C
PDF ISBN 978-92-846-6939-4|doi: 10.2861/880024|QA-04-20-418-EN -N

Специальная коллекция по искусственному интеллекту



Отказ от ответственности

Мнения, выводы, выводы и рекомендации, выраженные в данном документе, принадлежат авторам и не обязательно отражают взгляды и позиции Организации Объединенных Наций и ЮНИКРИ или любой другой соответствующей национальной, региональной или международной организации.

Содержание публикации может цитироваться или воспроизводиться при условии указания источника информации. Авторы не несут ответственности за возможное использование информации, содержащейся в этой публикации.

Используемое обозначение и представление материала в этой публикации не подразумевают выражения какого-либо мнения со стороны Секретариата Организации Объединенных Наций и ЮНИКРИ относительно правового статуса любой страны, территории, города или района или его властей, или в отношении делимитации его границ.

ЮНИКРИ обратился к авторам с просьбой провести глубокий анализ рассматриваемой темы, это не подразумевает какой-либо поддержки со стороны ЮНИКРИ и Секретариата ООН в отношении конкретных ссылок на государства-члены. Точно так же упоминание конкретных учреждений, компаний или продуктов определенных производителей не означает, что они одобрены или рекомендованы Секретариатом Организации Объединенных Наций или ЮНИКРИ по сравнению с другими аналогичными организациями, которые не упоминаются.

Благодарности

Эта Специальная коллекция по искусственному интеллекту была собрана г-жой Софи ван де Меуленграаф при поддержке г-на Одрана Маккарти и г-жи Аны Родригес Тамайо под общим руководством г-на Ираклия Беридзе. ЮНИКРИ хотел бы выразить свою признательность и поблагодарить всех авторов, которые внесли свой вклад в этот специальный сборник, а также внешних рецензентов, поддержавших этот процесс.

Авторские права

© Межрегиональный научно-исследовательский институт ООН по вопросам преступности и правосудия (ЮНИКРИ), 2020

Viale Maestri del Lavoro, 10, 10127 Турин, Италия

Тел .: + 39 011-6537 111/Факс: + 39 011-6313 368 Сайт: www.unicri.it

Электронная почта: unicri.publicinfo@un.org

Предисловие

Наш мир претерпевает масштабные технологические преобразования, затрагивающие все уровни общественной и частной жизни. В частности, разработки в области искусственного интеллекта (ИИ) бросают вызов традиционным перспективам, границам и методам и обещают повышение эффективности и результативности этого процесса. Подобно тому, как эта технология знаменует изменения в здравоохранении, розничной торговле, транспорте и финансовых услугах, достижения в области ИИ приближаются, и будут играть все более важную роль в предупреждении преступности и системе уголовного правосудия в предстоящие годы.

Подрывной характер этих технологий уже обсуждается в целом, но еще предстоит проделать большую работу, чтобы лучше понять изменения на горизонте и то, как заинтересованные сообщества и общество в целом могут подготовиться к ним, особенно с точки зрения адаптация и развитие политики и законодательства. Это влечет за собой не только понимание того, как формировать национальные и международные структуры управления, но также и то, как обеспечить их актуальность в свете темпов технологических инноваций. В то же время совершенно необходимо, чтобы мы лучше понимали, как защищать права человека и основные свободы с помощью таких рамок, поскольку, действительно, их уважение должно быть той самой основой, на которой мы работаем. Если ИИ нарушит эти правила, последствия будут далеко идущими, затронув жизнь людей и подорвав доверие общества к властям.

Несомненно, это захватывающее время, в которое мы находимся. Потенциал искусственного интеллекта для правоохранительных органов, юристов, судебной системы и даже в пенитенциарной системе огромен. Однако нам нужно будет по-настоящему проверить пределы нашего творчества и инноваций, чтобы преодолеть проблемы, связанные с этими технологиями, а также разработать совершенно новые подходы, стандарты и показатели, которые потребуются ими. Мы должны начать больше думать об этом и обо

всем диапазоне юридических аспектов ИИ, определить текущие варианты использования и возможные будущие сценарии и границы тестирования. В связи с этим на страницах этого Специального сборника ЮНИКРИ по искусственному интеллекту представлены избранные статьи, созданные новаторскими умами в академических кругах, и мы искренне надеемся, что этот сборник станет ценным вкладом. Мы надеемся, что эти статьи послужат стимулом для обсуждения в этой области и о том, как формировать структуру политики и правовых рамок будущего, и послужат руководством для тех, кто будет создавать соответствующие инструменты и методы на основе ИИ.

Тем не менее, я должен сделать вывод, подчеркнув, что ни один конкретный вариант использования ИИ, упомянутый в этой подборке, не должен восприниматься как одобрение со стороны ЮНИКРИ. Наше намерение состоит не в том, чтобы предлагать, для чего следует использовать ИИ, а в том, чтобы спровоцировать размышления, дискуссии и, возможно, даже возможные решения проблем, с которыми мы столкнемся в этой новой области.

Ираклий Беридзе



Руководитель, Центр ЮНИКРИ по искусственному интеллекту и робототехнике

Балансирующие испытания как инструмент регулирования искусственной разведки в области уголовного права

Франсиско Томас Рицци. Специалист по уголовному праву и магистр судебного права. Кандидат юридических наук. В настоящее время работает секретарем в Генеральной прокуратуре департамента Сан-Исидро, Буэнос-Айрес.

Агустин Пера. Юрист, с отличием окончил Университет Буэнос-Айреса (UBA), в настоящее время получает степень магистра уголовного права (UBA). Секретарь уголовного суда Буэнос-Айреса.

Краткий обзор

Появление новых технологий влечет за собой неоспоримые преимущества, хотя и с присущими им рисками. Проанализировав прошлый опыт, в данной статье предлагается, чтобы уголовное право как наука опиралось на вклад других наук, сохраняя, однако, его конституционную структуру. Что касается искусственного интеллекта, особенно когда внедрение систем с искусственным интеллектом вступает в противоречие с правами граждан, подчеркивается важность судебного контроля в конкретных случаях, а также то, как это осуществляется путем применения фильтра соразмерности, в котором права и принципы в конфликте взвешиваются. Наконец, в нем анализируется, как можно применять судебный контроль перед лицом внедрения некоторых систем искусственного интеллекта, обычно используемых в сфере безопасности и в юрисдикционных областях.

Ключевые слова: уголовное право, новые технологии, искусственный интеллект, судебный контроль, фильтр соразмерности, тест балансировки.

Вступление

Достижения в области искусственного интеллекта (ИИ)[237] ознаменовали смену парадигмы в развитии и изучении различных наук. Уголовное право не было исключением. Что касается безопасности, то возможность массового проведения сложных исследовательских исследований и разведывательных задач без ограничений, установленных законодательством, часто приводила к отсутствию надлежащего контроля, гарантирующего соблюдение прав человека.

Анализируя результат прошлого опыта, мы предлагаем способ осуществления судебного контроля в конкретном случае внедрения новых технологий в соответствии с существующими правовыми принципами, обеспечивая таким образом, чтобы рациональность не была упущена.

---

[237] Авторы хотели бы поблагодарить Клару Рицци за ее комментарии и предложения относительно написания настоящей статьи.

Как мы знаем, не существует единого принятого и жесткого определения ИИ; тем не менее, в данной статье мы будем говорить о системах ИИ в широком смысле. Европейский экономический и социальный комитет делит ИИ на узкий ИИ и общий ИИ: узкий ИИ способен выполнять определенные задачи, а общий ИИ способен выполнять любую умственную задачу, которую может выполнить человек. См. Catelijne Muller, «Европейский экономический

и социальный комитет. 526-е пленарное заседание EESC 31 мая и 1 июня 2017 г. »в Официальном журнале Европейского Союза, 08/2017: C 288 / 1–288 / 9, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016IE5369&from=EN

Эта основная идея утверждает, что ИИ должен работать как инструмент на службе человечества, а не как палка о двух концах, которая может обернуться против нас[238].

Уголовное право в области медицины и биологии

Как мы уже упоминали выше, в XIX веке влияние медицины и биологии на уголовное право привело к созданию новой школы, известной в континентальной Европе как специальная профилактика.

В этой области были разработаны терапевтические доктрины социальной защиты[239], как и в случае так называемой Scuola Positiva в Италии. Основными авторами которой были Чезаре Ломброзо, Энрико Ферри, Раффаэле Гарофало, Эудженио Флориан и Филипи Гриспиньи[240]. Медицинские разработки того времени, утверждали, что преступники были низшими существами, врожденными, извращенными в разной степени. Они пришли к выводу, что правонарушение может быть объяснено антропологически[241] и что наказание должно налагаться обществом для его собственной защиты, уступая место гигиенически-профилактическим мерам, терапевтическим и репрессивным или хирургическим-устраняющим мерам, в зависимости от каждого случая.

Точно так же были разработаны корректирующие доктрины, как в случае знаменитой Марбургской программы, запущенной в 1882 году немецким писателем Францем фон Листом, который постулировал, что наказание должно иметь немедленный эффект исправления, запугивания и нейтрализации.

Таким образом, наказание должно определяться по типу преступника:

- реабилитация дееспособных и исправных;
- отпугивание преступников, не нуждающихся в исправлении;
- недееспособность преступников, признанных неисправимыми[242].

В общем праве Джереми Бентам разработал теорию утилитаризма, в которой использовался «критерий полезности» в качестве руководства даже в

---

[238] Стивен Хокинг, Breves respuestas a las grandes preguntas (Буэнос-Айрес, Критика, 2019), 230-233. Стивен Хокинг указывает на важность заблаговременного планирования и предотвращения неотъемлемых рисков в отношении развития ИИ, поскольку обратное может привести к «худшему, что когда-либо могло случиться с человечеством», размышляя о мире со сверхразумным ИИ способен развивать своеволие, противоречащее нашему собственному.

[239] Luigi Ferrajoli, *Derecho y Razón* (Madrid: Editorial Trotta, 1997), 265.

[240] Ferrajoli, 266.

[241] Thomas Vormbaum, *Historia Moderna del Derecho Penal Alemán* (Valencia: Tirant Lo Blanch, 2018), 204

[242] Franz Von Liszt, *La idea de Fin en el Derecho Penal* (México: Universidad Nacional Autónoma de México y Universidad de Valparaíso de Chile, 1994), 112.

рамках концепции морали, согласно которой все действия можно было измерить на основе их результатов. Он считал, что наказание должно иметь двойную исправительную функцию: с одной стороны, влиять на общество, а с другой – исправлять преступника. Из этой идеи он впоследствии разработал свой знаменитый паноптикум[243].

В то время мировоззрение биолога и механиста возникло во всем мире, что привело к развитию теорий типа утилитаризма и поставило под угрозу, по крайней мере – давнюю кантовскую концепцию человека, как самоцели[244] начали применяться не пропорционально их виновности, а в соответствии с характером человека с учетом представляемой «опасности».

Эти теории возникли в основном из-за двух соперничающих интересов: ученого и политика. С одной стороны, только естественные науки и точные науки в то время считались актуальными «науками», а право воспринималось как ненаучная дисциплина. Эти авторы пытались обойти этот перекресток и снабдить право содержанием самых престижных наук, превратив его в точную науку. С другой стороны, на политическом уровне подчинение права точным наукам отвечало на то, что при этом время считалось ценностью: юридическая безопасность[245]. Не уступая никаким оценочным суждениям, Ло казалось защищался от всех видов манипуляций посредством интерпретации, гарантируя, что судья действительно может быть la bouche qui prononce les paroles de la loi[246], оставляя незатронутым поле действия законодательной власти.

Короче говоря, был сделан вывод о том, что из-за воздействия этих научных достижений на уголовное право последнее уступило им свою сущность и в какой-то момент утратило свою сущность; или, по крайней мере, отклонился от того направления, в котором он шел, когда его двигал идеализм, который поставил человека в центр уравнения[247]. Таким образом, понятие человеческого достоинства и уважение его свободы игнорировались в погоне за

---

[243] Joaquín Escriche, *Compendio de los Tratados de la Legislación Civil y Penal de Jeremías Bentham* (Madrid: Librería de la Viuda de Calleja e Hijos, 1839), 91; José Juan Moreso, *Jeremy Bentham: Luces y Sombras*, (Barcelona: Anales de la Catedra Francisco Suarez, 2013), 226.

[244] Immanuel Kant, *Fundamentación de la Metafisica de las Costumbres* (San Juan: Pedro M. Rosario Barbosa, 2007), 42.

[245] Santiago Mir Puig, "Límites del Normativismo en el Derecho Penal", *Imputación Objetivas y Dogmática Penal*, (Mérida: Universidad de los Andes, 2005), 31. Испанский автор объясняет, что в догме это имело конкретные последствия для континентальная теория преступности. С другой стороны, действие подразумевало только физическое движение, определяющее причинность результата. Антизаконность была простым описанием специально спланированной ситуации, а виновность была подтверждением психологической связи между фактом и разумом. Эти концепции, как таковые, лишены всякой социальной значимости, оценочных суждений и упрека, что привело к тому, что можно рассматривать как дегуманизацию процесса.

[246] Montesquieu, Del espíritu de las Leyes (Buenos Aires: Libertador, 2004), 137.

[247] Vormbaum, 196. In this respect, Vormbaum points out that the humanitarian aspiration of this illustration ceded in favour of a 'relentless science'.

изменение характера подсудимых или получение результата, полезного для остального общества[248].

Уголовное право и нейронауки

Достижения нейробиологии оказали аналогичное влияние на юридическую науку[249], из которых первый признак приписывается Бенджамину Либету в 80-х, который утверждал, что свобода воли была иллюзией[250]. Это уступило место новой концепции «детерминизма обновлений» и древняя дискуссия между детерминизмом и индетерминизмом была переиздана, что сегодня имеет серьезные последствия в отношении виновности.

Аналогичным образом, успехи в этой области, связанные с разработкой позитронно-эмиссионной томографии (ПЭТ), ядерного магнитного резонанса (RM или fMRI) и магнитоэнцефалографии, призваны опровергнуть теорию о том, что люди действуют свободно и добровольно, что само по себе Известно, что это предпосылка преобладающих тезисов о виновности: возможность поступить иначе как основание для порицания. Главный принцип концепции карающего правосудия заключается в том, что наказание оправдано в той мере,

---

[248] Фактически, абсолютизация этих теорий идет вразрез с реальной структурой современных демократий, в которых свобода и ответственность - как принцип виновности - конфигурируют ядерную характеристику. См. Бернардо Фейхоо Санчес, La pena como institución jurídica, (Buenos Aires: B de F, 2017), 156. Точно так же Эухенио Заффарони указывает, что криминальный материализм - биологические теории - формирует «бесчеловечное» уголовное право. См. Эухенио Рауль Заффарони, Tratado de Derecho Penal Parte General (Буэнос-Айрес: Ediar, 1998), 121. Кроме того, Феррахоли объясняет, что исправительные доктрины несовместимы с уважением к человеческой личности.
Он считает, что они идут вразрез с ценностями свободы и равенства, поскольку полагают, что правонарушители
- это неполноценные или ненормальные люди. Он утверждает, что рассмотрение уголовного обращения как абсолютизированной идеи наносит ущерб концепции человеческого достоинства и демократическому принципу уважения и терпимости к человеческой субъективности. См. Ferrajoli, 271.

[249] А также по смежным наукам, таким как нейрофилософия, философия разума и когнитивная психология.

[250] Таким образом, Герхард Рот утверждает, что произвольное действие, направленное «сознательным я», было иллюзией, поскольку было обнаружено, что вследствие соединения миндалевидного тела, гиппокампа, вентрального и дорсального узлов эмоциональная память опыт (который работает на бессознательном уровне) был тем, что определило принятие решения. Таким образом, у них будет место в лимбической системе за одну или две секунды до того, как они будут восприняты сознательно. Вольфганг Принц, со своей стороны, понимает свободную волю как социальный институт, который не соответствует научно доказуемой реальности с психической точки зрения. Вольф Зингер считает, что восприятие, которое мы воспринимаем как объективное, есть не что иное, как результат конструктивных процессов. Таким образом, как и в случае с поведением животных, человек полностью детерминирован, и каждое действие обязательно является результатом комбинации констелляции, которая дает начало настоящему стимулу, с непосредственно предшествующим состоянием мозга, определяемым генетической организацией, множество эпигенетических факторов и образовательных процессов, которые влияют на нервную цепь и, наконец, из-за непосредственного предшествующего анамнеза, динамическое взаимодействие нейронов, см. Eduardo Demetrio Crespo, “Compatibilismo Humanista: Una Propuesta De Conciliación Entre Neurociencias Y Derecho Penal” in Neurociencias y Derecho Penal, (Madrid: B de F, 2013).

в какой его исполнение компенсирует или, по крайней мере, не превышает ущерб, причиненный виновным в преступлении[251].

Это послужило источником так называемых «нейродетерминистских постулатов», в которых утверждалось, что правовой контроль правонарушений должен осуществляться путем вмешательства в мозг правонарушителей с помощью соответствующих «неврологических методов лечения»[252] или «улучшения»[253], а не с помощью наказания, основанного на их порицании. Другими словами, Правовая система лечебных мероприятий, а не наказаний по заслугам[254].

Возникли три разные позиции в отношении вторжения нейробиологии в уголовное право. Первый утверждает, что развитие этой науки не связано с уголовным правом, поскольку его объект определяется не научными знаниями, а нормативными понятиями, которые могут отличаться от эмпирических[255].

Второй защищает зависимость уголовного права от нейробиологических знаний и утверждает, что в настоящее время необходима трансформация для обоснования его целей[256]. Третий признает, что уголовное право не может игнорировать научные знания, и указывает, что оно не может повлечь за собой изменение модели его обоснования тоже. Согласно этой позиции криминалисты должны ценить научные знания во внимании к целям и функциям уголовного права[257].

---

[251] Mercedes Pérez Manzano, “Fundamento y fines del derecho penal. una revisión a la luz de las aportaciones de la neurociencia”, Indret: Revista para el Análisis del Derecho, 02/2011, https://indret.com/wp-content/themes/indret/pdf/818.pdf.

[252] Там же.

[253] Reinhard Merkel, “Novedosas intervenciones del Cerebro. Mejora de la Condición Humana Mental y Límites en el Derecho Penal”, Revista de Derecho Penal. Culpabilidad: Nuevas Tendencias l, No. 2, 2012 (Buenos Aires: Rubinzal Culzoni, 2013); Райнхард Меркель определяет «улучшение» как подходящую процедуру для создания ситуации, которая изменяется на физиологическом или ментальном уровне, что не может рассматриваться как лечебное лечение
и воспринимается как улучшение для человека
.

[254] Bernardo Feijoo Sánchez, “Derecho Penal y Neurociencias ¿Una relación tormentosa?”, Indret: Revista para el Análisis del Derecho, No. 1/2020, https://indret.com/?autor=bernardo-feijoo-sanchez

[255] Winfried Hassemer, “Neurociencias y culpabilidad en Derecho penal”, Indret: Revista para el Análisis del Derecho, No. 2, 2011; Günther Jakobs, “Culpabilidad Jurídico-Penal y Libre Albedrío” in Derecho Penal de Culpabilidad y Neurociencias, (Madrid: Thomson Reuters, 2012); Bernardo Feijoo Sánchez; Peter-Alexis Albrecht, “Culpabilidad: Restricciones al poder punitivo” in Culpabilidad: Nuevas Tendencias I (Buenos Aires: Rubinzal Culzoni, 2013), 31; Stephan Stübinger “¿Persona o Paciente? Comentarios sobre el Principio de Culpabilidad en el Derecho Penal desde el punto de vista de la investigación del cerebro” in Revista de Derecho Penal. Culpabilidad: Nuevas Tendencias l, No. 2, 2012); et al.

[256] Francisco Rubia, Neurociencia y Derecho penal: nuevas perspectivas en el ámbito de la culpabilidad y tratamiento jurídico-penal de la peligrosidad, comp. by Maroto Calatayud and Demetrio Crespo, (Madrid: B de F, 2013), 185-190.

[257] 21Pérez Manzano, “Fundamento y fines del derecho penal. una revisión a la luz de las aportaciones de la neurociencia”; Eduardo Demetrio Crespo, “Compatibilismo Humanista: Una Propuesta De Conciliación Entre Neurociencias Y Derecho Penal” in Neurociencias y Derecho Penal, (Madrid: B de F, 2013); Manuel Cancio Meliá, “Psicopatía y Derecho penal: algunas consideraciones introductorias”, Derecho Penal de Culpabilidad y Neurociencias (Madrid: Thomson Reuters, 2012).

Третья позиция, которую мы сочли правильной, была сначала принята в деле Роппер против Симмонса[258], а затем в деле Грэхем против Флориды[259] Верховным судом США[260].

В этих делах Суд опирался на научные достижения в области нейробиологии, чтобы продемонстрировать, что вина несовершеннолетних меньше, чем у взрослых, и на этом основании подтвердил, что они не могут нести такое же наказание в подобных случаях. Тем не менее, центральный пункт этого аргумента состоит в том, что правовая система использовала науку не для поддержки научно-биологической концепции, а для наполнения содержания нормативной концепции виновности; то есть не описывать это, а обрисовывать в общих чертах юридическую концепцию с учетом вклада нейробиологии, не раскрывая сущности самой концепции.

Уголовное право и появление искусственного интеллекта

Замечено, что в обоих случаях юридической науке пришлось столкнуться с научно-эмпирическими достижениями зарубежных наук, что вынудило ее пересмотреть центральные вопросы системы, последствия которых были замечательными.

Несмотря на результат первого опыта, появление редукционистских позиций в отношении человеческого поведения является выдающимся. Эти позиции, поддерживаемые теперь нейробиологами, предлагают правовую систему, но уже не наказаний, основанных на виновности, а лечебных мер, которые в какой-то момент напоминают Марбургскую программу[261]. Приняв иностранные заключения и перенеся их в правовую систему, как Винфрид Хассемер утверждал, что это была категорическая ошибка[262]. Несмотря на это,

---

[258] Roper v. Simmons, (543 U.S. 551, 2005).

[259] Graham v. Florida (560 U.S. 48, 2010); see also Cara H. Drinan, "Graham on the Ground" in Washington Law Review No. 87, (2012). 51.

[260] В деле Ропер против Симмонса суд проанализировал, было ли допустимо в соответствии с Восьмой и Четырнадцатой поправками к Конституции Соединенных Штатов казнить несовершеннолетнего правонарушителя старше 15, но моложе 18 лет, когда он совершил преступление, караемое смертной казнью, и виновность, как они подтвердили, «(…) респондент, проводивший научные и социологические исследования, и его друзья, как правило, подтверждают, что« [] недостаток зрелости и неразвитое чувство ответственности обнаруживаются у молодежи чаще, чем у взрослых, и их легче понять молодой. Эти качества часто приводят к стремительным и необдуманным действиям и решениям ». В деле Грэм против Флориды обсуждался вопрос о том, разрешает ли Конституция приговаривать несовершеннолетнего правонарушителя к пожизненному тюремному заключению без права досрочного освобождения за преступление, не являющееся убийством, и при такой возможности, они указали, что «(…) достижения в психологии и науке о мозге продолжают выявлять фундаментальные различия между сознанием подростков и взрослых. Например, части мозга, участвующие в управлении поведением, продолжают развиваться в позднем подростковом возрасте (…) ».

[261] Feijoo Sánchez, 10.

[262] Hassemer, "Neurociencias y culpabilidad en Derecho penal", 6. Бывший судья Конституционного суда Германии объяснил, что категорическая ошибка проистекает из нарушения принципа знания и теории науки, то

было бы также ошибкой игнорировать научные достижения и рисовать юридическую науку, совершенно не связанную с ними.

В этом смысле мы понимаем, что путь, по которому идет третья позиция, предлагающая использовать необработанные данные для достижения юридических целей, является наиболее вероятным вариантом. Наша позиция в отношении ИИ основана на этой идее.

Научные достижения должны быть адаптированы к уголовному праву[263], а не наоборот. Иными словами, они должны быть интегрированы таким образом, чтобы они не препятствовали правовой основе, построенной вокруг уважения прав человека[264].

Было бы трудно представить, как ИИ повлияет на эту область права в будущем, но, точно так же, как он мог использовать точные, биологические и технологические науки, не отказываясь от своей цели, мы понимаем, что это будет также возможно контролировать использование ИИ путем установления правовых норм и принципов[265].

Однако из-за того, что нет надлежащих правил для внедрения ИИ в глобальном масштабе[266], это не может привести к неограниченному разрешению на его реализацию без какого-либо контроля. Нет сомнений или,

---

есть все науки могут видеть только то, что их инструменты позволяют им видеть и находить ответы, тогда как их инструменты позволяют им формулировать вопросы, соответствующие категоричному ответу. Инструменты каждой науки определяются их формальным объектом, и он контролируется системой, основанной на долге, парадигмами, методами и инструментами. Таким образом, науки, основанные на эмпирических методах, не смогут судить, существует ли, например, «свобода».

[263] Мы ссылаемся на Уголовное право в объективном смысле: «ряд правовых норм, оценок и принципов, которые препятствуют совершению преступлений и запрещают их и связаны с ними, например, бюджет, наказание и / или меры безопасности как правовые последствия». See Santiago Mir Puig, Derecho Penal, Parte General, (Barcelona: Ed. Reppertor. 2006) 45. Кроме того, когда мы говорим о правовых нормах, их следует понимать в глобальном смысле, включая уголовно-процессуальное право, закон о наказаниях, пенитенциарные учреждения. юриспруденция, ювенальное уголовное право и криминология. See Claus Roxin, Derecho Penal Parte General Tomo I. Fundamentos. La estructura de la teoría del delito (Madrid: Civitas, 1997), 44.

[264] В этом смысле Хассемер относится к науке об уголовном праве, ориентированной на последствия. Это означает, что законодатель, органы уголовного правосудия и тюремная администрация не удовлетворены судебным преследованием и компенсацией за счет искупления правонарушителя, но их цель - улучшить положение правонарушителя и сдержать правонарушение в целом. See Winfried Hassemer, Fundamentos del Derecho Penal, (Barcelona: Bosch, 1984) 35. Следует добавить, что фактическая законность Уголовного закона подтверждается одобрением в соответствии с Конституцией. See Günther Jakobs, Derecho Penal. Parte General (Madrid: Marcial Pons, 1997) 44.

[265] Следует отметить, что в уголовном праве предусмотрены более жесткие наказания за нанесение вреда нормативным требованиям. Это настолько опасно, что цивилизованные общества должны обеспечивать их различными способами и защищать их от попадания в чужие руки, а также следить за тем, чтобы они использовались осторожно, одинаково и соразмерно. See Winfried Hassemer, Crítica al Derecho Penal de Hoy, (Buenos Aires: Editorial Ad.Hoc., 1995) 19. Из этого следует, что все ограничивающие принципы ius punendi играют фундаментальную роль, позволяя рационализировать их использование в демократических рамках. See Santiago Mir Puig, Derecho Penal, Parte General, (Barcelona: Reppertor, 2006) 104.

[266] Аналогичным образом Специальный докладчик Филип Олстон призвал к регулированию ИИ для обеспечения соблюдения прав человека и к переосмыслению позитивных способов, с помощью которых цифровое государство всеобщего благосостояния могло бы стать движущей силой для создания значительно улучшенных систем социальная защита (Филип Алстон, «Крайняя бедность и права человека», доклад, представленный в соответствии с резолюцией 35/19 Совета по правам человека, Генеральная Ассамблея ООН).

по крайней мере, не должно быть, что мы можем потребовать от нашего правительства соблюдения минимального стандарта реализации при использовании ИИ в государственной политике[267]. Насколько мы понимаем, такой стандарт может быть найден в надлежащем отношении права человека, требующие разумного внедрения технологий в рамках верховенства закона[268].

Одна из проблем, с которыми мы сталкиваемся, заключается в том, что мы не учитываем, по крайней мере, на данный момент, способ пересечения аксиологических ценностей с точными единицами значений, которые могут быть введены внутри алгоритма, или метод сопряжения в нем каких-либо ссылок на принципы. Такая проблема находится не в технических областях, а в самой юридической науке: право не может точно определить стоимость юридических активов, и его философия не может также зафиксировать аксиологический вес ценностей и принципов в математических терминах[269]. По этой причине мы считаем что системы искусственного интеллекта для принятия судебных решений не способны дать правовой ответ на сложные дела[270], не впадая в бентанский утилитаризм.

Следуя вышесказанному, для целей Закона ИИ может рассматриваться только как внешний инструмент. Ввиду большого количества разрабатываемых систем ИИ не только в отношении безопасности, но и юрисдикции, мы понимаем, что установление пределов их использования является необходимостью. Пока такие ограничения не регулируются законом, их применение должно проверяться в конкретных случаях с помощью эффективного судебного контроля[271].

Закон имеет ряд инструментов, позволяющих определить, когда норма схожа с правовой системой. Что касается систем искусственного интеллекта, то целью его внедрения правительством является повышение эффективности в сфере безопасности.

---

[267] По словам Дворкина, если мы не можем требовать от правительства предоставления адекватных решений по правам граждан, мы можем потребовать, чтобы они, по крайней мере, сделали все возможное для этого: «(…) мы можем потребовать, чтобы они серьезно относились к правам». See Ronald Dworkin, Los Derechos en serio, (Barcelona: Ariel Derecho, 2010) 278.

[268] Бернардо Фейхоо Санчес справедливо указывает, что конституционный закон требует соотношения легитимности и эффективности таким образом, чтобы неэффективный инструмент или, в его случае, неэффективный, терял свою легитимность, принимая во внимание затраты с юридической точки зрения. See Bernard Feijoo Sánchez, La pena como institución jurídica, (Buenos Aires: B de F, 2017) 92.

[269] Таким образом, Винфрид Хассемер и Франсиско Муньос Конде подчеркивают, что уважение человеческого достоинства - это юридическая ценность, не допускающая какой-либо экономической количественной оценки или обмена с другими ценностями. See Winfried Hassemer, Francisco and Muñoz Conde, Introducción a la Criminología y al Derecho Penal (Valencia: Tirant Lo Blanch, 1989), 101.

[270] Чтобы найти определение, относящееся к такого рода случаям, можно обратиться к работе Дворкина. Ronald Dworkin, Los Derechos en serio, (Barcelona: Ariel Derecho, 2010), 146.

[271] Мы должны прояснить, что мы имеем в виду правовой контроль над административными и судебными решениями, но не законодательный судебный контроль, который Джереми Уолдрон определил как «строгий судебный контроль», который поставил под сомнение свои принципы. See Jeremy Waldron, Contra el Gobierno de los Jueces, (Buenos Aires: Siglo Veintiuno, 2018), 61.

Задачи, балансирующие тесты[272] становится особенно интересным. Это происходит из-за того, что коллективные блага[273] вступают в игру против индивидуальных прав[274], требуя точки пропорционального баланса между преимуществами первых и влиянием вторых. Балансировка – чрезвычайно полезный правовой метод разрешения конфликта интересов, который узаконивает его вмешательство в права и принципы[275].

Тест на равновесие возник в качестве аргументационной техники соразмерности, разработанной Конституционным судом Германии[276], а затем эмигрировал в другие конституционные суды, чтобы окончательно утвердиться в качестве инструмента передового опыта в международной системе прав человека. Это очень полезный метод при определении того, становится ли влияние индивидуального права непропорциональным в погоне за коллективным благом. Он импортирует способ материализации из принципа соразмерности[277]. Этот принцип, который стал одним из столпов современного права[278], а также краеугольным камнем многочисленных теорий уголовного права[279]. Однако, следует применять осторожно, поскольку, как указывает Гюнтер Якобс, это слишком формальная концепция[280], которая должна быть наполнена рассматриваемыми оценками и, в этом смысле, позволять вводить субъективные вопросы оператора[281].

---

[272] Следует отметить, что для анализа коллизии между индивидуальными правами и коллективными благами необходимо, во-первых, рассчитывать на принципы теории индивидуальных прав или принимать их во внимание. Это означает понимать принципы как мандаты оптимизации в противоположность правилам, подразумеваемым в определенном мандате (как предложено Робертом Алекси - see Robert Alexy, El Concepto y la Validez del Derecho, (Barcelona: Gedisa, 2004) 161); или же дихотомия между правами и принципами (как предлагает Рональд Дворкин - see Dworkin, 32).

[273] Хотя определить коллективные блага непросто, можно констатировать, что, по словам Роберта Алекси, если речь идет о товарах, структура которых не является распределительной (т.е. не может быть распределена между гражданами) и имеет нормативный статус (т.е. правовая система); и обоснованы в правиле, которое, по мнению Алексия, эти правила должны быть обоснованы в консенсусной теории истины. See Alexy, 179.

[274] Согласно теории Дворкина, понимаются как «политические права», базовые или институциональные, но имеющие силу против решений большинства. (see Dworkin, 37); понимается как «права как полномочия по оптимизации», согласно Алексию (see Alexy, 185); или понимаются как «права, основанные на идее личной автономии», т е. принцип, в соответствии с которым предписывается максимизация способности людей выбирать и материализовывать жизненный идеал, согласно Карлосу Нино (See Carlos Nino, Una teoría de la justicia para la democracia. (Buenos Aires: Siglo Veintiuno, 2013) 127).

[275] Winfried Hassemer, Crítica al Derecho Penal de Hoy, 64. Хассемер считает его даже «сильным инструментом».

[276] See Elena Bindi, "Test de proporcionalidad en el age of balancing", UNED Revista de Derecho Político, No. 96, 05/2016. https://doi.org/10.5944/rdp.96.2016

[277] Robert Alexy, Teoría de la Argumentación Jurídica. La teoría del discurso racional como teoría de la fundamentación jurídica (Lima: Palestra, 2010) 459.

[278] Это принцип, согласно которому любое вмешательство государства, затрагивающее права граждан, должно быть ограничено. Он предполагает конституционное требование, когда в уголовном праве вмешательство государства затрагивает основные права. See Santiago Mir Puig, Derecho Penal, Parte General, (Barcelona: Reppertor, 2006) 127.

[279] See Von Hirsch's work in the United States, Andrew Von Hirsch, Censurar y Castigar, (Madrid: Trotta, 1998) 31; or Hörnle's work in Germany, Tatjana Hörnle, Determinación de la Pena y Culpabilidad, (Buenos Aires: FD, 2003) 81.

[280] Günther Jakobs, Derecho Penal. Parte General, (Madrid: Marcial Pons, 1997) 568.

[281] Следует отметить, что его формальность, хотя она может быть опасной, поскольку позволяет вводить субъективные оценки, при правильном использовании также может быть динамическим принципом, поскольку может принимать социальные изменения и ценности каждого конкретного общества.

Что касается испытания на балансировку, то наиболее технически разработанная разработка была сделана в основном Робертом Алекси, который изложил «формулу взвешивания». Алекси полагал, что соразмерность имеет три субпринципа: принципы пригодности, необходимости и соразмерности в более узком смысле.[282] Последний является тем, который нас больше всего беспокоит, поскольку он относится исключительно к правовым возможностям. В этом подпринципе возникла концепция балансировки. Согласно этой теории, перед фундаментальными правами, правило гласит, что: чем больше степень неудовлетворения или ущерба одному принципу, тем важнее должно быть соблюдение другого.[283]

Если взять вышеупомянутое в нашу предметную область, это будет включать определение того, какие права должны быть защищены, а какие права должны быть затронуты при использовании эффективной программы AI. Таким образом, предлагается три шага: а) определить степень влияния одного из принципов или прав; б) оценить важность удовлетворения противоположного принципа/права; в) определить, насколько важен противоположный принцип / право оправдывает ограничение первого. Шкала интенсивности (легкая, умеренная и тяжелая) была создана для измерения веса вмешательства и степени важности, которая его оправдывает.[284] Эти шаги продемонстрируют, может ли программа ИИ применяться рационально и, следовательно, применима ли она с соблюдением этических норм. параметры.[285] Короче говоря, эта процедура предлагает проанализировать, оправдано ли нарушение прав человека степенью вмешательства систем ИИ в общество. Разумно полагать, что для того, чтобы гарантировать надлежащее осуществление прав граждан и чтобы они были максимально эффективными, необходимо, чтобы каждый отказался от возможности осуществления этого или любого другого права. Точно так же люди должны отказываться от индивидуальных прав,

---

[282] Alexy, 458. В аналогичном смысле Хассемер называет этот третий подпринцип «исполнимостью». Однако он признает, что это последний компонент принципа, согласно которому закон может действовать только в том случае, если запрет или мандат подлежат исполнению. См. Уинфред Хассемер, «Принципиальной пропорции комо лимите де лас интервенционес юридико пеналес» в уголовном деле Лимитеса аль Деречо. Principios operativos en la foundationación del castigo, (Барселона: Ателье, 2012), 195.

[283] Alexy, 460. Следует уточнить, что для немецкого автора основные права имеют структуру принципов и составляют мандат оптимизации.

[284] Алексий, 462. Мы понимаем, что измерение будет зависеть от ценностей и идеалов каждого конкретного общества, и даже несмотря на то, что существуют глобальные соглашения относительно важности соблюдения определенных принципов защиты прав человека, оно не всегда будет одинаковым в каждом конкретном обществе. общества или конкретной страны, в связи с особенностями или конкретными потребностями каждого региона. Мы считаем, что лучший способ добиться правильного измерения - это процедуры юридической аргументации, такие как представленные Alexy; или коллективное обсуждение, которое Карлос Нино называет «эпистемологическим конструктивизмом». См. Карлос Нино, Una teoría de la justicia para la democracia, (Буэнос-Айрес: Siglo Veintiuno, 2013), 89. В этом смысле Алекси указывает, что легитимность веса в законе зависит от его рациональности.

[285] См. Судебное решение Межамериканского суда по правам человека по делу Киммел против Аргентины; а также Европейский суд по правам человека, бельгийские языковые меньшинства, 23 июля 1968 г.

чтобы гарантировать коллективные блага.[286] Однако это регулирование не должно приводить к чрезмерной аффектации, когда главная цель не пропорциональна влиянию индивидуального права. Таким образом, масштабное вторжение может быть оправдано только тогда, когда продемонстрирован, несомненно властный интерес.[287] Дворкин указывает, что мы должны признать, что у правительства есть причина для ограничения прав, если оно правдоподобно считает, что конкурирующее право более важно[288] и что курс правительства состоит в том, чтобы придерживаться середины, уравновешивать общее благо и личные права, отдавая каждому должное.[289] По словам Мануэля Атьензы, речь идет не об изобретении закона, а о его развитии[290]. Это то, что мы предлагаем чтобы справиться с применением ИИ в вопросах профилактики.

Применение балансировочных тестов

Ниже мы укажем, как тесты балансировки могут применяться для анализа реализации систем ИИ.

Во-первых, мы рассмотрим PredPol.[291]. Эта система представляет собой систему прогнозирующего наблюдения, которая проецирует на карту места и время вероятного совершения конкретных преступлений, позволяя эффективно распределять ресурсы для их предотвращения.[292]

Тем не менее, первое, что мы можем отметить в этой программе это то, что её использование может привести к стигматизации определенных областей за более высокий уровень преступности[293]. Принимая во внимание шаги

---

[286] Dworkin, 289. Точно так же Джон Ролз указывает, что, ограничивая свободу, чтобы гарантировать равные условия для всех граждан, то есть от имени общих интересов, правительство действует по принципу, который будет выбран в «исходной позиции» (Мексика : Fondo de Cultura Económica, 2006), 203.

[287] Таким образом, Американская конвенция о правах человека «Пакт Сан-Хосе, Коста-Рика» устанавливает личные обязанности в статье 32 под названием «Взаимосвязь между обязанностями и правами»

[288] Дворкин, 288.

[289] Дворкин, 294.

[290] Мануэль Атьенса, «Constitucionalismo y Derecho Penal» в Конституции и системе наказания, (Мадрид: Marcial Pons, 2012), 35.

[291] См. Веб-сайт Predpol: https://www.predpol.com/. Этот робот был создан в рамках исследовательского проекта, который проводился Департаментом полиции Лос-Анджелеса и Калифорнийским университетом в Лос-Анджелесе с целью извлечения выгоды из информации, полученной в результате заявленных преступных действий.

[292] Эта система использует три конкретных вида информации (вид уголовного преступления, место и время совершения преступления), которые вводятся в математический алгоритм, который анализирует их, чтобы предсказать, какие районы города являются наиболее проблемными, и на основе этого организует полицию. патрулирование маршрутов с целью усиления профилактики в наиболее опасных зонах. Этот подающий надежды алгоритм работает, связывая определенные виды преступного поведения с математической структурой, чтобы определить эволюцию преступных моделей.

[293] Мария Эрнандес Хименес, «Inteligencia Artificial y Derecho Penal», в Actualidad Jurídica Iberoamericana, № 10, июнь 2019 г. 817.

Алекси, легко заметить, что цель программы – усилить полицейский контроль в определенных областях. В определенных областях это приведет к увеличению числа задержаний, реквизиций и т.д. Представьте себе это в этом смысле, учитывая предложенную автором триадную шкалу, что можно установить, что упомянутое вторжение – умеренно применяемое и соблюдающее личные гарантии – подразумевает среднее ущемление прав людей, проживающих в беднейших районах. С другой стороны, принимая во внимание противоположный принцип, можно также установить, что существует особый интерес к защите конкурирующего права на безопасность, насколько это возможно. Возвращаясь к шкале, представьте, что можно установить, что незащищенность представляет собой чрезвычайно серьезную угрозу. В этом отношении и с учетом третьего шага можно сделать вывод, что, хотя неравномерное ограничение свободы и неприкосновенности частной жизни является значительным, более важно гарантировать безопасность в тех областях, которые затронуты преступной деятельностью. Следовательно, аффектация пропорциональна степени важности ее удовлетворения, поэтому использование такой системы, как Predpol, может быть хорошо сбалансированным.

Во-вторых, мы проанализируем системы, призванные помочь легальному труду, среди которых остановимся на COMPAS[294]. Это программное обеспечение использует алгоритмы для оценки риска потенциальных рецидивов. Он задуман как полезный инструмент для судей при принятии ими судебных решений[295].

Внедрение этой системы было объектом критики, среди которой выделяются следующие: а) из-за того, что алгоритмы являются коммерческой тайной, не было раскрыто, как на самом деле работает система, что ограничивает осуществление права на защиту, что влияет на надлежащий процесс; [296]б) учитывая, что система опирается на то, чему ее учит программист, демонстрируя, например, расистские тенденции, они будут затронуты в ее функции, что приведет к возможной пристрастности; [297]и в)

---

[294] (Профили управления исправительными правонарушителями для альтернативных санкций).

[295] Выводы были основаны на ответах на 137 вопросов о конкретных обстоятельствах каждого правонарушителя, включая всю информацию, связанную с их судимостями. Точная цифра была получена в результате расследования, проведенного Джулией Дрессел и Хани Фарид, «Точность, справедливость и пределы прогнозирования рецидивизма», Sci. Adv. 2018; 4: eaao5580 17 января 2018 года; и статья Эда Янга «Популярный алгоритм не лучше предсказывает преступления, чем случайные люди» в The Atlantic, 17 января 2018 г. (https://www.theatlantic.com / технология / архив / 2018/01 / эквивалент-COMPAS-алгоритм / 550646 /). См. Также Мария Эрнандес Хименес, «Inteligencia Artificial y Derecho Penal» в «Actualidad Jurídica Iberoamericana», № 10, июнь 2019 г. 817.

[296] См. Дело штата Висконсин против Эрика Л. Лумиса (2015AP157-CR, 2016). Этот вопрос был передан на рассмотрение Верховного суда Висконсина Соединенных Штатов.

[297] Эрнандес Хименес, «Inteligencia Artificial y Derecho Penal», 824-825. Чтобы подтвердить то, что там раскрыто, см. Джулия Ангвин и другие, «Machine Bias», в ProPublica, 23 мая 2016 г., https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal -предложение.

система не является более точной, чем прогнозы, сделанные людьми с небольшим опытом или без опыта в уголовном правосудии: действительно, линейная система, использующая только два параметра (возраст и количество судимостей), даст почти те же результаты.[298]

Исходя из вышеизложенного, разумно отметить, что, хотя необходимо найти меры, способствующие уменьшению ошибок и судебного произвола, мы находимся в наличии инструмента, пригодность которого обсуждается, и его следует должным образом отсортировать, чтобы продвигайтесь с тестом на балансировку. Однако для целей нашего упражнения, если возможно преодолеть упомянутое препятствие, будут отмечены неблагоприятные результаты для его реализации. Фактически, обращая особое внимание на первого показанного критика, легко обнаружить, что программа подразумевает вторжение вправо на защиту, поскольку, как уже упоминалось, она не раскрывает, как достигаются результаты, препятствуя его контролю.[299] С этой целью можно утверждать, что вторжение осуществляется «серьезным» субъектом[300]. Что касается противоположного принципа, соответствующие решения имеют тенденцию, в общих чертах, к реализации целей наказания. Точнее, что делает их профилактическими. Тем не менее, следует отметить, что эта процедура не обозначена как необходимая для всех целей, а просто представляет собой еще один инструмент для вмешивающегося судьи. В этом смысле можно сделать вывод, что внедрение этой системы не оправдывает ограничения такого масштаба права на защиту; следовательно, поскольку невозможно проверить наличие пропорциональности, можно сделать вывод,

---

[298] Джулия Дрессел и Хани Фарид, «Точность, справедливость и пределы прогнозирования рецидивизма», Science Advances, 17 января 2018 г.

[299] В совместном отчете ЮНИКРИ и Интерпола об искусственном интеллекте и робототехнике для правоохранительных органов установлено, что для уважения основных прав граждан и избежания потенциальной ответственности их использование в правоохранительных органах должно характеризоваться следующими характеристиками: справедливость, подотчетность, прозрачность и способность действовать. объяснил.

При объяснении концепции прозрачности было оговорено, что путь, выбранный системой для достижения определенного вывода или решения, не должен быть «черным ящиком», и, принимая во внимание возможность объяснения, они заверили, что решения и действия системы должны быть понятны для пользователей (UNICRI-INTERPOL, Искусственный интеллект и робототехника для правоохранительных органов, доклад, представленный

2 апреля 2019 г. на заседании высокого уровня: Искусственный интеллект и робототехника - изменение будущего преступности, терроризма и Безопасность). Аналогичным образом Специальный докладчик Филип Олстон заявил,

что общественность должна иметь возможность понимать и оценивать политику, скрытую глубоко внутри алгоритмов (Филип Олстон, «Крайняя бедность и права человека», отчет, представленный в соответствии с Human Резолюция Совета по правам 35/19, ООН - Генеральная Ассамблея).

[300] См. Дело Штат Висконсин против Эрика Л. Лумиса, чтобы найти определенные аргументы, способствующие смягчению этого вторжения, например: i) что COMPAS не предсказывает конкретную вероятность рецидива правонарушителя, но результаты получены путем сравнения ситуации тот человек с группой аналогичных случаев; ii) что в отчете, выпущенном COMPAS, указаны некоторые элементы, взвешенные с учетом возможности их оспаривания. Однако верно то, что судья и стороны не знают с точностью ни всех рассмотренных параметров, ни того, как на самом деле работает система. Это может усугубиться, если действительно удастся установить остальные приписываемые недостатки.

что не рекомендуется применять такую систему, как COMPAS, как она была представлена здесь [301].

Несмотря на критику, упомянутую в предыдущем абзаце, следует отметить, что она может ослабнуть в связи с PSA [302], алгоритмом, разработанным Фондом Лауры и Джона Арнольдов, целью которого является упорядочение использования предварительного заключения. По сути, эта система пытается определить по шкале от 1 до 6, насколько вероятно, что обвиняемый стал виновным в совершении новых преступлений, и насколько вероятно, что он не будет обращать внимания на цитаты, требуемые правосудием. Для получения этих результатов эта программа использует девять параметров, включая текущий возраст человека. Его предыдущие судимости, невыполненный приговор, неявку в суд, а с другой стороны, оставляет в стороне все вопросы, связанные с рассой, полом, должностями и уровнем образования[303]. При публикации совокупности факторов, уравновешивающих получение результатов, эта система выделяется тем, что позволяет оспаривать их. Следовательно, влияние рассматриваемого права могло быть уменьшено, что в конечном итоге изменило окончательный результат уравнения, предложенного Алексием, и возможность обоснования его реализации.

Следует отметить, что приведенные примеры не являются исчерпывающим анализом, а являются лишь иллюстрацией того, как следует проводить испытание на балансировку. Для того чтобы иметь возможность выполнять масштабную задачу, необходимо собрать статистические данные с большей точностью, чтобы проанализировать их глубже, что выходит за рамки цели настоящей статьи.

В дополнение к упомянутым системам Окружной суд Гааги недавно вынес решение по так называемому «делу SyRI» [304], в котором судьи заявили, что право на неприкосновенность частной жизни преобладает над охотой против предполагаемых мошенников. SyRI [305] был разработан Министерством социальных дел Нидерландов в 2014 году для выявления тех, кто с наибольшей

---

[301] Следует напомнить, что проведенная оценка тесно связана с ценностями и идеалами каждого конкретного общества, резюмированными в различных действующих правовых системах, что может фактически склонить чашу весов к приемлемости или неприемлемости исследуемой системы. . Следует отметить, что во время вынесения решения по делу «Лумис» Суд штата Висконсин начал его рассмотрение, особо сославшись на намерение разработать механизмы для консолидации общественной безопасности, укрепляя доминирование рассматриваемых принципов.
В указанном заявлении была подтверждена возможность того, что судья может использовать этот инструмент, даже если с определенными ограничениями и с определенными предупреждениями.

[302] Оценка общественной безопасности. См. Веб-сайт оценки общественной безопасности https://www.psapretrial.org/about.

[303] Эрнандес Хименес, «Inteligencia Artificial y Derecho Penal», 826-827.

[304] NJCM CS / De Staat der Nederlanden. В этом деле Специальный докладчик Филип Олстон представил в качестве amicus curiae также вывод о том, что СИРИ представляет значительную потенциальную угрозу правам человека,
в частности, для самых бедных слоев общества.

[305] Индикатор системного риска.

вероятностью совершит мошенничество против социальной системы с целью получения государственных пособий. Это приложение для профилирования рисков. Суд установил, что правительство Нидерландов не смогло найти баланс между правом на неприкосновенность частной жизни и общественными интересами при обнаружении мошенничества в сфере социального обеспечения, и, таким образом, использование SyRI несоразмерно цели, которую оно стремилось достичь[306].

Случай SyRi показал, что действительно возможно управлять технологией искусственного интеллекта при условии, что мы правильно используем закон, поставив права человека в центр уравнения. Путем правильного баланса между затронутыми правами и преимуществами систем ИИ можно определить, используется ли ИИ в качестве инструмента на службе человечества или, наоборот, в качестве оружия против нас.

Вывод

Появление систем, которые собирают, обрабатывают, анализируют и интерпретируют быстро большие объемы информации, является реальностью, которая, несомненно, несет важные преимущества, хотя и с определенными рисками. Среди которых мы должны подчеркнуть следующее: а) их внедрение дает определенные фундаментальные результаты в области прав человека непропорционально сильно пострадали; б) они могут быть потенциально использованы преступными или террористическими группами; в) на более апокалиптическом уровне их безрассудное развитие может привести к точке невозврата, которая может поставить под угрозу выживание человечества. Мы понимаем, что во избежание любого из упомянутых результатов необходимо учитывать новаторские правила и эффективный судебный контроль, чтобы обеспечить ответственное развитие этих новых технологий.

Ввиду вышеизложенного, приспосабливаясь не только к нашей реальности, но и к цели настоящей статьи, мы вкратце предлагаем попытаться извлечь выгоду из прошлого опыта и разработать метод, по крайней мере,

---

[306] При применении теста балансировки учитывались следующие факторы: а) обработка данных в SyRi затронула значительную часть населения; б) что оно было направлено на обездоленные группы граждан (понимая, что это нарушает запрет на дискриминацию по статье 14 и право на уважение частной жизни по статье 8, как из Европейской конвенции о правах человека); с) что была проведена перекрестная проверка данных, взятых из нескольких источников; г) цели программы и категория используемой информации были широкими и расплывчатыми; е) что отчеты о рисках уступают место важным санкциям; и е) что результаты были малопригодны. На основании вышеизложенного был сделан вывод, что развертывание, необходимое для реализации SyRi, было непропорциональным.

чтобы иметь возможность бороться с синдицированными рисками как отправной точкой.

Анализируя, как эмпирические науки влияли на закон в 19 веке, мы пытались сформулировать идею о том, что научные достижения не могут определить закон, чтобы поставить под угрозу его сущность. Напротив, мы понимаем, что право, а точнее уголовное право, должно использовать и использовать весь вклад других наук, в то же время, сохраняя свою конституционную структуру.

Прояснив эту идею, мы должны быть предельно осторожны с внедрением систем с искусственным интеллектом, которые могут противоречить правам граждан, с единственным оправданием повышения производительности и эффективности. Более того, мы понимаем, что каждый из них, в спорных случаях, должен пройти судебный фильтр пропорциональности, в котором их отношения с правами или с конфликтующими принципами анализируются, определяя степень аффектации одной стороны и необходимость удовлетворения другой стороны, чтобы окончательно установить, действительно ли цель оправдывает вмешательство.

Как следствие, несмотря на отсутствие регулирования, обеспечивающего определенную безопасность, мы считаем, что посредством надлежащего использования судебных инструментов можно руководить и контролировать использование систем ИИ в рамках пути, отмеченного сильной правовой базой. Насколько мы понимаем, это единственный способ, которым эта технология может стать опорой эволюции человечества.

Ссылки

Хирш, Эндрю Фон, Censurar y Castigar (Мадрид: Trotta, 1998).

Фейхоо Санчес, Бернардо, La pena como institución jurídica, (Буэнос-Айрес: B de F, 2017).

Фейхоо Санчес, Бернардо, «Derecho Penal y Neurociencias ¿Una relación tormentosa?», Indret: Revista para el Análisis del Derecho, № 1/2020, https://indret.com/?autor=bernardo-feijoo-sanchez.

Дринан, Кара Х., «Грэм на земле» в Washington Law Review № 87 (2012).

Нино, Карлос, Una teoría de la justicia para la democracia. (Буэнос-Айрес: Сигло Вейнтиуно, 201.

Мюллер, Кателийне, «Европейский экономический и социальный комитет. 526-е пленарное заседание EESC 31 мая и 1 июня 2017 г. »в Официальном журнале Европейского Союза, 08/2017: C 288 / 1–288 / 9, https://eur-lex.europa.eu/legal-content/EN / TXT / PDF /? Uri = CELEX: 52016IE5369 & from = EN.

Роксин, Клаус, Derecho Penal Parte General Tomo I. Fundamentos. La estructura de la teoría del delito (Мадрид: Civitas, 1997)

Креспо, Эдуардо Деметрио, «Compatibilismo Humanista: Una Propuesta De Conciliación Entre Neurociencias Y Derecho Penal» в Neurociencias y Derecho Penal, (Мадрид: B de F, 2013).

Бинди, Елена, «Проверка пропорциональности возраста балансирования», UNED Revista de Derecho Político, № 96, 05/2016. https://doi.org/10.5944/rdp.96.2016

Заффарони, Эухенио Рауль, Tratado de Derecho Penal Parte General (Буэнос-Айрес: Ediar, 1998).

Рубиа, Франсиско, Neurociencia y Derecho штраф: новые перспективы en el ámbito de la culpabilidad y tratamiento jurídico-Pen de la peligrosidad, comp. Марото Калатаюд и Деметрио Креспо, (Мадрид: B de F, 2013).

Лист, Франц Фон, La idea de Fin en el Derecho Penal (Мексика: Национальный автономный университет Мексики и университет Вальпараисо де Чили, 1994).

Якобс, Гюнтер, «Culpabilidad Jurídico-Penal y Libre Albedrío» в Derecho Penal de Culpabilidad y Neurociencias, (Мадрид: Thomson Reuters, 2012)

Якобс, Гюнтер, Деречо Пенал. Parte General (Мадрид: Marcial Pons, 1997)

Кант, Иммануэль, Fundamentación de la Metafísica de las Costumbres (Сан-Хуан: Педро М. Росарио Барбоса, 2007).

Уолдрон, Джереми, Contra el Gobierno de los Jueces, (Буэнос-Айрес: Siglo Veintiuno, 2018).

Эскриче, Хоакин, Compendio de los Tratados de la Legislación Civil y Penal de Jeremías Bentham (Мадрид: Librería de la Viuda de Calleja e Hijos, 1839).

Ролз, Джон, Теория де ла Justicia (Мексика: Fondo de Cultura Económica, 2006).

Моресо, Хосе Хуан, Джереми Бентам: Люс и Сомбрас, (Барселона: Аналес де ла Катедра Франсиско Суарес, 2013).

Ангвин, Джулия и другие, «Machine Bias», в ProPublica, 23 мая 2016 г.

Дрессел, Джулия и Фарид, Хани, «Точность, справедливость и пределы прогнозирования рецидивизма», Sci. Adv. 2018; 4: eaao5580 17 января 2018 г.

Феррахоли, Луиджи, Деречо и Разон (Мадрид: Эдиториал Тротта, 1997).

Атьенса, Мануэль, «Конституционализм и Деречо уголовное наказание» в Конституции и системе уголовного наказания (Мадрид: Marcial Pons, 2012).

Кансио Мелиа, Мануэль, «Psicopatía y Derecho Penal: algunas consideraciones Introductionctorias», Derecho Penal de Culpabilidad y Neurociencias (Мадрид: Thomson Reuters, 2012).

Эрнандес Хименес, Мария, «Inteligencia Artificial y Derecho Penal», в Actualidad Jurídica Iberoamericana, № 10, июнь 2019 г.

Перес Манзано, «Мерседес»: «Фундаментальные и штрафные санкции». una revisión a la luz de las aportaciones de la neurociencia », Indret: Revista para el Análisis del Derecho, 02/2011, https://indret.com/wp- content / themes / indret / pdf / 818.pdf.

Монтескье, Del espíritu de las Leyes (Буэнос-Айрес: Libertador, 2004).

Альбрехт, Петер-Алексис, «Culpabilidad: Restricciones al poder punitivo» в Culpabilidad: Nuevas Tendencias I (Буэнос-Айрес: Rubinzal Culzoni, 2013).

Олстон, Филип, «Крайняя бедность и права человека», отчет, представленный в соответствии с резолюцией 35/19 Совета по правам человека, Генеральная Ассамблея ООН.

Меркель Рейнхард, «Novedosas intervenciones del Cerebro. Mejora de la Condición Humana Mental y Límites en el Derecho Penal », Revista de Derecho Penal. Culpabilidad: Nuevas Tendencias l, No. 2, 2012 (Буэнос-Айрес: Rubinzal Culzoni, 2013).

Алекси, Роберт, Эль концепция и ла Валидес дель Деречо, (Барселона: Гедиса, 2004).

Алексий, Роберт, Теория де ла Аргументасьон Юридика. La teoría del discurso racional como teoría de la foundationación jurídica (Лима: Палестра, 2010).

Дворкин, Рональд, Los Derechos en serio, (Барселона: Ариэль Деречо, 2010).

Мир Пуиг, Сантьяго, «Límites del Normativismo en el Derecho Penal», Imputación Objetivas y Dogmática Penal, (Мерида: Universidad de los Andes, 2005).

Мир Пуч, Сантьяго, Derecho Penal, Parte General, (Барселона: Ред. Реппертор, 2006).

Штюбингер, Стефан «Persona o Paciente? Comentarios sobre el Principio de Culpabilidad en el Derecho Penal desde el punto de vista de lavestigación del cerebro »в Revista de Derecho Penal. Culpabilidad: Nuevas Tendencias l, No. 2, 2012).

Хокинг, Стивен, Breves respuestas a las grandes preguntas (Буэнос-Айрес, Критика, 2019).

Хёрнле, Татьяна, Determinación de la Pena y Culpabilidad, (Буэнос-Айрес: FD, 2003).

Формбаум, Томас, Historia Moderna del Derecho Penal Alemán (Валенсия: Тирант Ло Бланш, 2018).

ЮНИКРИ-ИНТЕРПОЛ, «Искусственный интеллект и робототехника для правоохранительных органов», доклад был представлен 2 апреля 2019 г. на заседании высокого уровня: «Искусственный интеллект и робототехника – меняя будущее преступности, терроризма и безопасности». Хассемер, Уинфред, «Принципиальной пропорции комо лимите де лас интервенционес юридико пеналес» в пенитенциарной системе Лимитеса аль Деречо. Principios operativos en la foundationación del castigo, (Барселона: Ателье, 2012).

Хассемер, Винфрид, «Neurociencias y culpabilidad en Derecho Penal», Indret: Revista para el Análisis del Derecho, № 2, 2011.

Хассемер, Винфрид, Критика аль Деречо Пенал де Хой, (Буэнос-Айрес: от редакции Ad.Hoc., 1995).

Хассемер, Винфрид и Муньос Конде, Франсиско, Introducción a la Criminología y al Derecho Penal (Валенсия: Tirant Lo Blanch, 1989).

Хассемер, Винфрид, Fundamentos del Derecho Penal, (Барселона: Bosch, 1984).

Справедливость, доверие и технология лица в полисировании

Эмили Джонсон, Антони Наперальски, Зига Скорьянц [307]

Глобальное распространение и использование технологий распознавания лиц правоохранительными органами справедливо вызвало неоднозначные чувства у публики, которую опрашивают специалисты. В этой статье

[307] Авторы - младшие научные сотрудники факультета инноваций и цифровизации права Венского университета, Австрия.

утверждается, что отсутствие доверия является следствием отсутствия регулирования. Как показано в этом документе, доверие по своей сути связано с принципом справедливости защиты данных Европейского Союза (ЕС), поскольку суть справедливости – это доверие. Чтобы компенсировать недостаток доверия, мы предлагаем использовать принцип справедливости в качестве политического ориентира при регулировании технологии распознавания лиц. В этом материале представлено двойственное отношение общества к использованию технологий распознавания лиц полицией во всем мире. После этого принцип «справедливости» подвергается деконструкции и затем применяется в качестве потенциального помощника в укреплении доверия к технологиям распознавания лиц и новым технологиям в целом.

Ключевые слова: доверие, распознавание лиц, принципы, защита данных.

Вступление

Внедрение технологии распознавания лиц (FRT) растет во всем мире, и ожидается, что ее рыночная стоимость вырастет с 3,2 миллиарда долларов в 2019 году до 7 миллиардов долларов в 2024 году. С этим, казалось бы, неизбежным увеличением FRT возникает неизбежная обеспокоенность неправильным использованием данных о лицах. Неудивительно, что опасения связаны с уникальной и конфиденциальной природой данных о лицах, а также с простотой использования в сочетании с возможностью неправильного использования данных.

Неудивительно, что ответные меры против ФРТ последовали. Макияж против распознавания лиц, камуфляж, прически[308], маски[309] и очки[310] – всё это материализовалось как реакция на угрозу публичного применения FRT. Понятно, что существуют оговорки относительно юридических параметров (или их отсутствия) использования FRT. Что касается использования технологий на базе искусственного интеллекта, было отмечено, что «[любая] тенденция слепо верить в то, что на самом деле остается в значительной степени ненадежной технологией, может привести к ошибочным, а иногда и опасным выводам»[311]. FRT. Поскольку FRT является технологией, несущей повышенный риск массового наблюдения, доверие проистекает из надежности

[308] «CV Dazzle: камуфляж от распознавания лиц».
[309] Джип ван Левенштейн, «Исключение наблюдения».
[310] Кикучи, «Козырек конфиденциальности препятствует технологии распознавания лиц».

[311] Херлберт, «Сколько можно доверять искусственному интеллекту?»

и точности самой технологии, а также её ответственного, справедливого и прозрачного развертывания[312].

«Рынок распознавания лиц по программному обеспечению и услугам – 2024 Marketsand Markets».

Как заявил Елинек: «Без гарантии того, что защита личных данных соблюдается, не будет доверия к технологии»[313]. Следуя этому подходу, как утверждается в этом материале, для укрепления доверия к таким спорным технологиям, как FRT, необходимо регулирование присутствовать и иметь исковую силу в пользу защиты основных прав и свобод граждан. В настоящее время в ЕС или на международном уровне мало регулирования, прямо ориентированного на FRT. Однако правила и принципы защиты данных в ЕС обеспечивают основу для соответствующего направления будущего законодательства. Тем не менее, мы не намерены анализировать проблемы соблюдения нормативных требований. Скорее, эта глава сосредоточена на предоставлении руководящих принципов, которые будут способствовать разработке справедливого регулирования FRT.

В следующем материале рассматривается недостаток общественного доверия[314], представленный FRT, и то, как этот недостаток доверия можно смягчить путем реализации некоторых давних принципов защиты данных. Этот вклад будет не просто оценивать соответствующие принципы защиты данных как закон с черной буквы, но скорее как более широкие руководящие принципы политики для регулирования новых и потенциально инвазивных технологий. Для начала, этот вклад представляет текущий уровень доверия и отношения к FRT в различных международных условиях. Исходя из этого, в данной публикации исследуется, как всеобъемлющий закон, содержание которого основано на фундаментальных принципах защиты данных и конфиденциальности, может укрепить доверие к защите данных. Чтобы оценить этот момент, в данной публикации анализируются случаи, когда укоренившиеся правовые и социальные принципы служили источником права в прошлом, а затем последующее международное и глобальное влияние, связанное с этой формой регулирования. Затем этот вклад более конкретно фокусируется на принципе законности, справедливости и прозрачности, а также на том, где и почему этот принцип может помочь повысить уровень доверия к FRT. В этой статье в конечном итоге утверждается, что регулирование может

---

[312] Брэдфорд и др., «Живое распознавание лиц».
[313] «EDPB в Твиттере».
[314] «Ограничения британской общественности на использование технологии распознавания лиц»; «За пределами номинальной стоимости».

быть источником справедливости и доверия, а отсутствие регулирования в значительной степени способствует отсутствию доверия к FRT.

А что насчет доверия?

Поскольку FRT все чаще используется во всем мире, в следующем разделе будет изучено отношение граждан к FRT в ряде мест.

В недавней Белой книге Европейской комиссии по ИИ, совершенству и доверию в Европе утверждается, что использование распознавания лиц в общественных местах угрожает достоинству людей из-за возможного вмешательства вправо на уважение частной жизни и защиту личных данных. В контексте правоприменения должно соблюдаться строгое соблюдение принципов необходимости и соразмерности, а также принцип разрешения со стороны законодательства ЕС или национального законодательства в сочетании с соответствующими гарантиями[315].

Институт Ады Лавлейс, независимый исследовательский орган, работающий над тем, чтобы данные и ИИ работали на людей в обществе, провел первое общенациональное исследование общественного мнения о FRT в Великобритании[316]. Исследование пришло к выводу, что «[t] здесь не является поддержкой полиции в развертывании технологии распознавания лиц»[317] до такой степени, что «55% людей считают, что правительство должно ограничить использование полицией функции распознавания лиц конкретными обстоятельствами»[318]. Сценарий использования полицейскими технологии распознавания лиц»[319]. Причины дискомфорта по поводу использования FRT полицией варьировались от опасений по поводу конфиденциальности, нормализации технологий наблюдения, отсутствия вариантов отказа или согласия и общего недоверия к использованию полицией FRT этично[320]. Эти общественные мнения небезосновательны. Независимый обзор использования FRT полицией MET показал, что существовала неадекватная правовая основа для использования технологии и невыполнение требования необходимости, и, следовательно, потенциальное нарушение закона об основных правах[321].

---

[315] «Белая книга по искусственному интеллекту»; Хартия основных прав Европейского Союза.
[316] «Превышение номинальной стоимости».
[317] Там же, 2.
[318] Там же, 10.
[319] Там же, 11.
[320] Там же.
[321] Фасси и Мюррей, «Независимый отчет об испытании столичной полиции Лондона технологии распознавания лиц».

Изучая США, исследование Pew Research Center16 в 2019 году показало, что большинство опрошенных американцев «доверяют правоохранительным органам ответственно использовать распознавание лиц, но общественность менее доверяет[322] рекламодателям и технологическим компаниям»[323]. 59% опрошенных проголосовали за то, что правоохранительные органы могут использовать технологию распознавания лиц при оценке угроз безопасности в общественных местах. Для сравнения, только 15% заявили, что рекламодатели могут использовать эту технологию в общественных местах для отслеживания реакции на публичные показы рекламы. Интересно, что исследование также выявило различия между демографическими группами: сравнительно меньшая часть молодых людей доверяет распознаванию лиц правоохранительными органами в общественных местах. Хотя это исследование демонстрирует общую поддержку и доверие к использованию FRT правоохранительными органами, 40% опрошенных не верят, что правоохранительные органы используют FRT ответственно.

В Германии материализовались планы министра внутренних дел Хорста Зеехофера по широкому использованию FRT в аэропортах и на вокзалах в качестве шага по внесению поправок в закон о федеральной полиции для улучшения технических возможностей полиции и расширения их ответственности[324]. Ответ групп активистов включал полный запрет государства на использование FRT в общественных местах[325].

После COVID-19 китайские компании начали выпускать улучшенный FRT, который может «обнаруживать повышенную температуру в толпе или отмечать граждан, не носящих лицевую маску»[326]. Эта информация распознавания лиц затем передается в приложения, чтобы предупреждать пользователей. Область личной информации о здоровье других, чтобы установить, были ли они в непосредственной близости от инфицированных пациентов. Хотя нет поддающегося проверке обзора отношения китайских граждан к их общему чувству доверия, отдельные граждане выразили обеспокоенность тем, что правительство находит больше причин для публичного наблюдения за своими гражданами[327]. Публичные действия в ответ на ФРТ также демонстрирует отсутствие доверия и даже неприязнь к ФРТ со стороны правительства. В Гонконге протестующие разрушили башни

---

[322] Смит, «Более половины взрослых в США доверяют правоохранительным органам ответственно использовать распознавание лиц».
[323] Там же
[324] Грюль, «Планы Германии по автоматическому распознаванию лиц встречают жесткую критику».
[325] Там же.
[326] Куо, «Новая нормальность».
[327] Там же.

распознавания лиц в знак протеста, полагая, что в них находится китайский FRT[328].

В то время как части обществ, которые обсуждали, доверяют использованию ФРТ в полиции, доверие общества остается неполным, а проблемы многочисленны. Учитывая, что FRT – это технология слежки, она рассматривалась как источник недоверия и вторжение в частную жизнь. В качестве средства обеспечения доверия и достаточного регулирования тех, кто стоит за FRT, в этом документе рассматривается принцип справедливости в защите данных, чтобы внести определенный вклад в устранение проблем и их источников, а также в конечном итоге поощрить доверие.

Правовые принципы: ответ на недостаток доверия

Поскольку проблемы, связанные с отсутствием доверия общества к FRT, носят глобальный характер, при поиске возможного решения необходимо учитывать международную перспективу. В этой статье утверждается, что фундаментальные принципы закона о защите данных потенциально могут стать руководящими принципами глобальной политики для регулирования новых технологий. Хотя каждый из шести принципов защиты данных, несомненно, важен для защиты прав и интересов субъекта данных, в этом документе утверждается, что принцип «справедливости», изложенный в статье 5 (1) (a) GDPR[329] и статье 4 (1) (a) Директива 2016/68024, в частности, может иметь более широкое значение, чем просто регулирование обработки персональных данных в ЕС.

Как утверждается в этом документе, принцип справедливости способствует укреплению доверия между контроллером и субъектами данных, обязывая (будущих) диспетчеров разрабатывать и выполнять обработку в интересах своей собственной подотчетности и ответственности перед субъектами данных[330]. Если этот принцип используется как часть директивы политики (в отличие от правовой нормы), он может оказать существенное влияние на глобальном уровне в пользу более эффективного использования новых технологий и, следовательно, повышения общественного доверия.

---

[328] Доффман, «Гонконг обнажает обе стороны безжалостной машины распознавания лиц Китая».

[329] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46 / ЕС (Общие правила защиты данных) (текст, имеющий отношение к ЕЭЗ).

[330] Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовные преступления или исполнение уголовных наказаний, а также о свободном перемещении таких данных, а также об отмене Рамочного решения Совета 2008/977 / JHA.

Однако прежде всего необходимо установить, в чем именно заключается смысл принципа справедливости. Для этого в первую очередь нужно отличить его от других принципов защиты данных.

Отличие справедливости от других принципов защиты данных

Принцип справедливости обычно называют частью триады принципов. Статья 5 (1) (a) GDPR объединяет принципы законности, справедливости и прозрачности в одну общую единицу. Такой комбинированный подход вызывает сомнения относительно того, насколько принцип справедливости отделен от связанных с ним принципов. Однако, как утверждают ученые: «систематический и телеологический анализ статьи 5 (1) (a) GDPR требует, чтобы это положение рассматривалось как представляющее три различных, но частично совпадающих принципа»[331]. Это, на наш взгляд, убедительная интерпретация и может быть подтверждена выводами следующего анализа.

Клиффорд и Ослоос утверждают, что принципы справедливости всегда были тесно связаны[332]. Идя еще дальше, Краненборг указывает, что прозрачность является элементом справедливой обработки данных[333]. Эти аргументы можно проследить до формулировки статьи 5 (1) (a) GDPR, где принцип справедливости сопровождается принципами законности и прозрачности.

Тем не менее, в стипендии было указано, что рассмотрение обязанностей контролера в качестве основы принципа справедливости является результатом отсутствия четкого принципа прозрачности в Директиве 95/46/EC[334]. Таким образом, Суд Европейского Союза Европейского Союза (далее CJEU), необходимого для толкования обязанностей контролера по прозрачности исходя из принципа справедливости[335]. Тем не менее, в GDPR, прозрачность стала самостоятельным принципом (или, по крайней мере, имеет право на отдельное упоминание в законодательном текст) [336]. Таким образом, справедливость может (и должна), в свою очередь, рассматриваться как нечто большее, чем просто требование информирования субъекта данных о способах обработки данных, влияющих на него. Решение законодателей ввести прозрачность и справедливость в текст законодательства противоречит толкованию справедливости как прозрачности.

---

[331] Клиффорд и Ослоос, «Защита данных и роль справедливости», 159.
[332] Там же, 138.
[333] Краненборг, «Статья 8 - Защита личных данных», 254.
[334] Директива 95/46 / ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных.
[335] Росснагель, «Артикель 5», п. 45.
[336] Клиффорд и Ослоос, «Защита данных и роль справедливости».

Значение принципа справедливости

После устранения наиболее запутанного совпадения принципов справедливости и прозрачности в этом разделе подробно рассматривается значение принципа справедливости. Хотя очевидно, что справедливость применялась и интерпретировалась во множестве областей исследований (от политической или юридической философии до исследований в области управления)[337], этот вклад следует интерпретациям справедливости, доступным в стипендии о защите данных.

Хотя было заявлено, что «справедливость предполагает моральный COMPAS, чувство справедливого общества»[338], точное определение и значение принципа справедливости остается одним из самых загадочных в европейском законодательстве о защите данных. В рамках ЕС этот принцип можно найти в Хартии основных прав Европейского Союза (далее Хартия), в GDPR и в Директиве 2016/68033 (далее «Директива о правоприменении» или «LED»)[339]. Однако точное значение принципа справедливости (частично из-за широкого значения слова «справедливый»), тем не менее, может быть интерпретировано по-разному.

Для начала важно отметить, что «справедливость», как автономная концепция права ЕС, не может быть истолкована ссылкой на значение, приписываемое справедливости в национальных правовых системах[340]. Скорее, ради единого применения во всем ЕС, необходимо толковать этот термин по отношению к всеобъемлющей системе права ЕС. Поэтому первым делом следует обсудить буквальное значение этого термина.

Как определено в словаре английского языка Коллинза, «легкость – это качество разумности, правильности и справедливости»[341]. Многокомпонентное буквальное определение справедливости получило дальнейшее развитие благодаря исследованиям в области защиты данных. После сравнительного лингвистического анализа термина «справедливость» и изучения более широких национальных и культурных интерпретаций в различных

---

[337] Ролз, «Справедливость как честность»; Харт, «Есть ли естественные права?»; Клоско, «Принцип справедливости
и политических обязательств»; Филлипс, «Теория заинтересованных сторон и принцип справедливости»; Ван Бюрен, «Если проблема - справедливость, то решение - это согласие?

[338] Франк, Справедливость в международном праве и институтах, 7–8.

[339] Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовные преступления или исполнение уголовных наказаний, а также о свободном перемещении таких данных, а также об отмене Рамочного решения Совета 2008/977 / JHA.

[340] Kramer, Art. 5 ', п. 12; Росснагель, «Артикель 5», п. 46; Хербст, Искусство. 5 ДС-ГВО ', п. 13.

[341] «Определение и значение справедливости | Словарь английского языка Коллинза».

лингвистических версиях GDPR, Мальжери определил три ключевых значения, к которым относятся различные переводы слова «справедливость»: лояльный, равноправный и правильный[342]. Можно отметить значительное несоответствие между значением слова «справедливость», определенным в английском словаре, и тем, как оно используется в GDPR и переведено по всей Европе. Единственное совпадение между ними – это аспект правоты / справедливости. Или, проще говоря: поступать правильно. Однако концепция справедливого / правильного / равноправного может меняться с течением времени[343]. Таким образом, понятие «справедливость», очевидно, является субъективным понятием, но оно состоит из похожих и частично совпадающих интерпретаций, возникающих в результате перевода и интерпретации язык и, без сомнения, культурное и правовое развитие часто зависит от каждой национальной среды.

Следуя Мальджери, суть принципа справедливости заключается в «существенном смягчении несправедливого дисбаланса, создающего ситуации уязвимости»[344]. Справедливость не столько сосредоточена на соблюдении процедурных требований GDPR (таких как прозрачность или законность), но и скорее затрагивает суть властных отношений между контроллером и субъектом данных[345]. Аналогичное замечание сделано Clifford & Ausloos, которые утверждают, что принцип справедливости должен «сбалансировать асимметричные отношения между субъектом данных и контроллером»[346]. Этот аргумент предполагает, что справедливость помогает «предотвратить несправедливый дисбаланс между субъектами данных и контроллерами данных»[347]. В том смысле, что справедливость помогает поддерживать баланс между субъектом данных и контроллером, справедливость играет роль всеобъемлющего, но отдельного принципа в GDPR; это линза, через которую следует оценивать деятельность по обработке данных[348].

Этот вклад основан на различии, проведенном Clifford & Ausloos между явным и неявным смыслом принципа справедливости в защите данных[349]. По их мнению, принцип справедливости неявно защищает субъектов данных от злоупотреблений со стороны контроллеров[350]. Это коррелирует с явным значением принцип справедливости, направленный на предотвращение любого обмана субъектов данных в отношении «характера и целей операций обработки»[351]. Кроме того, замечания Мальжери позволяют отступить от узкого

---

[342] Мальджери, «Концепция справедливости в GDPR», 27–30.
[343] Bygrave, Закон о защите данных, 58.
[344] Мальджери, «Концепция справедливости в GDPR».
[345] Там же.
[346] Клиффорд и Ослоос, «Защита данных и роль справедливости», 159.
[347] Мальджери, «Концепция справедливости в GDPR»,
[348] Клиффорд и Ослоос, «Защита данных и роль справедливости», 159.
[349] Там же, 138.
[350] Там же, 140.
[351] Там же.; см. также Bygrave, Закон о защите данных, 58.

толкования законодательства о защите данных, расширяя его до более широкой проблемы регулирования технологий.

Следуя Хербсту, Росснагелю или Мальджери, в этом материале утверждается, что простое соблюдение GDPR и других правовых положений не всегда может быть достаточным для предотвращения квалификации операции обработки данных как нарушающей принцип справедливости[352]. Скорее, это общий (im) баланс сил между субъектом данных и контролером, который требует тщательной оценки в свете принципа справедливости[353]. Если субъект данных окажется в невыгодном положении из-за обработки данных каким-либо образом из-за отсутствия баланса сил (который сочтет необходимым для GDPR), даже если никакая другая норма не нарушена, обработка будет квалифицирована как нарушение принципа справедливости и, следовательно, незаконная[354].

Основываясь на вышеупомянутых аргументах, мы хотим пойти еще дальше и использовать принцип справедливости в качестве стандарта, регулирующего политику в области правоприменения во всем мире. Как правильно указал Росснагель, недобросовестное поведение – это просто поведение, нарушающее доверие субъекта данных[355]. Поэтому мы стремимся ввести принцип справедливости в качестве всемирно признанного метода смягчения недоверия к полицейской деятельности. При этом мы утверждаем, что наличие принципа справедливости (как он понимается на основании GDPR) в регулировании поощряет довер ие. Посредством минимизации (IM) баланса сил между контроллером и субъектом данных, подчинение принципу справедливости позволяет снизить риски, связанные с обработкой, как спорные, так как использование FRT данных. Его кросс-секционный характер позволяет оценивать обработку данных с более широкой точки зрения и обеспечивает соблюдение других принципов защиты данных.

Последний фрагмент анализа, который необходим в этом контексте, – это глобальные условия принципа справедливости в его нынешнем виде.

Таким образом, в следующем разделе анализируется место справедливости в некоторых ключевых глобальных и национальных инструментах и подходах к регулированию технологий.

---

[352] Herbst, Art. 5 ДС-ГВО ', п. 47.
[353] Там же.
[354] Там же.
[355] Росснагель, «Артикель 5», п. 47.

Справедливость как мировой стандарт

В международном праве справедливость можно рассматривать как «критерий дискурсивного управления [...] напряжением»[356]. Пример этого международного стандарта справедливости можно увидеть в годовом отчете Совета ООН по правам человека на тему: «Право на неприкосновенность частной жизни в эпоху цифровых технологий», в котором говорится, что справедливость является основным компонентом, составляющим минимальные стандарты обработки персональных данных[357]. Еще одним примером справедливости как глобального стандарта является статья 5 Конвенции 108 Совета Европы, которая заявляет, что «персональные данные, подвергающиеся автоматической обработке, должны: a) быть получены и обработаны справедливо и законно»[358]. Более того, в отношении модернизации Конвенции 108, статья 5 расширена в отношении «[l] законности обработки данных и качества данных», Где говорится, что при обработке персональных данных должен соблюдаться справедливый баланс между интересами заинтересованных сторон на всех этапах обработки[359]. Включение требования о том, что должна быть справедливая Баланс здесь говорит о растущем признании необходимости включения и применения принципа справедливости в защите данных на международном уровне.

Организация экономического сотрудничества и развития (ОЭСР) утверждает, что на основе «принципа ограничения сбора» должны быть ограничения на сбор персональных данных, требующие, чтобы данные были получены законными и справедливыми способами[360]. Уточнить значение слова «справедливый» в контексте защиты данных.

С национальной точки зрения, в Великобритании ICO выделяет три требования при оценке справедливости обработки данных:

1. Как обработка данных может повлиять на заинтересованных лиц и может ли быть оправдано любое неблагоприятное воздействие?

2. Вся обработка соответствует ожиданиям субъекта данных. Любая обработка, не отвечающая ожиданиям, должна быть оправданной.

---

[356] Франк, Справедливость в международном праве и институтах, 7.

[357] «Право на неприкосновенность частной жизни в эпоху цифровых технологий». Доклад Верховного комиссара ООН по правам человека».

[358] Совет Европы, Конвенция о защите частных лиц в отношении автоматической обработки персональных данных.

[359] Совет Европы, Конвенция 108+ о защите частных лиц в отношении автоматической обработки персональных данных.

[360] ОЭСР, Руководящие принципы защиты конфиденциальности и трансграничных потоков персональных данных.

3. Субъектов данных нельзя вводить в заблуждение или вводить в заблуждение при сборе и обработке данных[361].

Эти критерии подчеркивают влияние субъекта данных, его ожидания и доверия.

Общество юристов Шотландии заявляет, что «[в] для справедливой обработки личных данных обработка должна соответствовать ожиданиям субъекта данных»[362]. Это заявление возвращает нас к понятию справедливости и прозрачности. Субъект данных может формировать ожидания и питать доверие, если он прозрачен в намерениях и применении FRT. Если затем использование FRT будет справедливо в соответствии с ожиданиями субъекта данных, это может вызвать доверие к технологии.

Выводы

Справедливость – это ключевой принцип, который, если он применяется в контексте FRT, предлагает снизить риски, связанные с точностью, достоверностью, безопасностью, предвзятостью, дискриминацией, конфиденциальностью и прозрачностью – все это способствует общему (не) балансу сил между контроллером и субъектом данных.

Общественное недоверие к FRT присутствует. Хотя это недоверие, несомненно, связано с природой и характеристиками FRT, который часто рассматривается как инвазивный и тайный, значительный элемент этого недоверия, возможно, связан с отсутствием регулирования и последующему регламентированному применению FRT. Анализируя принципы «справедливости» в защите данных и применяя их к использованию FRT, мы находим расширение проверки качества закона в том смысле, что для «справедливого» развертывания FRT и обработки полученных биометрических данных, от тех, за кем ведется наблюдение, не обязательно требовать информирования об отдельных случаях и расследованиях. Это может быть практически невозможно для правоохранительных органов, но общественность должна знать об этой технологии в первую очередь. В этом случае необходимо знать типы технологий, кто их использует, где они используются, как данные собираются, обрабатываются и хранятся. Кроме того, правила обмена данными с третьими лицами или их использования в других целях также должны быть четкими и прозрачными. В конечном итоге, правила развертывания FRT

[361] ICO, «Принцип (a)».
[362] «Справедливая и прозрачная обработка».

должны быть четко прописаны. Применяя принцип справедливости в этом контексте, субъекты данных также должны иметь возможность оспаривать FRT и/или иметь возможность полагаться на надзорный орган.

Такой подход способствует справедливости и одновременно законности и прозрачности.

Результатом, который, безусловно, будет приветствоваться, будет четкое регулирование, приводящее к подотчетности контролеров за обработку с использованием FRT; как следствие, это привело бы к более высокому уровню доверия со стороны общественности. С этой точки зрения данная статья просто знаменует собой первый шаг в укреплении общественного доверия к новым технологиям со стороны правоохранительных органов. В будущих исследованиях необходимо будет изучить тест для оценки справедливости (или ее отсутствия) каждый раз, когда внедряются новые и инновационные технологии, направленные на оказание помощи правоохранительным органам.

Ссылки

«За пределами номинальной стоимости: отношение общества к технологии распознавания лиц». По состоянию на 14 марта 2020 г.

https://www.adalovelaceinstitute.org/beyond-face-value-public-attitude-to-facial-recognition-technology/.

Брэдфорд, Бен, Джулия Есберг, Джонатан Джексон и Пол Доусон. «Живое распознавание лиц: доверие и легитимность как предикторы общественной поддержки использования новых технологий полицией». Препринт. SocArXiv, 10 января 2020 г. https://doi.org/10.31235/osf.io/n3pwa.

Фонд Наффилда. Ограничения британской общественности на использование технологии распознавания лиц», 9 сентября 2019 г.

https://www.nuffieldfoundation.org/news/british-public-want-restrictions-on-the-use-of-facial-recognition-technology.

Бигрейв, Ли А. Закон о защите данных: подход к его обоснованию, логике и ограничениям. Серия законов об информации 10. Гаага; Нью-Йорк: Kluwer Law International, 2002.

Хартия основных прав Европейского Союза, 326 OJ C § (2012).

Клиффорд, Дамиан и Джеф Ослоос. «Защита данных и роль справедливости». Ежегодник европейского права 37 (1 января 2018 г.): 130–87.

https://doi.org/10.1093/yel/yey004.

Совет Европы. Конвенция 108+ о защите частных лиц при автоматической обработке персональных данных (2018 г.).

Конвенция о защите частных лиц в отношении автоматической обработки персональных данных, Pub. L. No. Серии европейских договоров - № 108 (1981).

«CV Dazzle: камуфляж от распознавания лиц». По состоянию на 14 марта 2020 г. https://cvdazzle.com/.

Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования преступников. правонарушений или исполнения уголовных наказаний, а также о свободном перемещении таких данных, а также об отмене Рамочного решения Совета 2008/977 / JHA, Pub. L. No. OJ L 119 p. 89–131. По состоянию на 12 августа 2019 г. https://eur-lex.europa.eu/eli/dir/2016/680/oj.

Доффман, Зак. «Гонконг демонстрирует обе стороны безжалостной машины распознавания лиц Китая». Forbes. По состоянию на 14 марта 2020 г.

https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/.

Twitter. 'EDPB в Twitter: «Председатель EDPB для @EP_Justice:« Каждый раз, когда личные данные обрабатываются в контексте борьбы с COVID-19, правила защиты данных незаменимы. Без гарантии того, что защита личных данных соблюдается, нельзя будет доверять этой технологии ».

https://t.co/f7HXX0TpMz / Twitter '. По состоянию на 16 мая 2020 г. https://twitter.com/EU_EDPB/status/1258428969965281280.

«Рынок распознавания лиц по программному обеспечению и услугам - 2024 г.|MarketsandMarkets». По состоянию на 14 марта 2020 г.

https://www.marketsandmarkets.com/Market-Reports/facial-recognition-market-995.html.

Юридическое общество Шотландии. «Справедливая и прозрачная обработка». По состоянию на 14 марта 2020 г. https://www.lawscot.org.uk/members/business-support/gdpr-general-data-protection-regulation/gdpr-guide/create-a-record-of-data-processing/fair -и-прозрачная-обработка /.

'Определение и значение справедливости | Словарь английского языка Коллинза ». Доступ 8 марта 2020 г.

https://www.collinsdictionary.com/dictionary/english/fairness.

Франк, Томас М. Справедливость в международном праве и институтах. Перепечатано. Оксфорд: Oxford Univ. Пресса, 2002.

Фасси, Питер и Дараг Мюррей. «Независимый отчет об испытании технологии распознавания лиц в режиме реального времени, проведенного Столичной полицейской службой Лондона», 2019 г. http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech

Грюль, Филипп. «Планы Германии по автоматическому распознаванию лиц встречают жесткую критику». Www.Euractiv.Com (блог), 10 января 2020 г.

https://www.euractiv.com/section/data-protection/news/german-ministers-plan-to-expand-automatic-facial-recognition-meets-fierce-criticism/.

Харт, HLA «Есть ли естественные права?» Философское обозрение 64, вып. 2 (1955): 175–91. https://doi.org/10.2307/2182586.

Хербст, Тобиас. 'Искусство. 5 ДС-ГВО '. В Datenschutz-Grundverordnung / BDSG. Комментарий, отредактированный Юргеном Кюлингом и Бенедиктом Бухнером, 2-е изд., 2018.

Херлберт, Джордж. «Насколько можно доверять искусственному интеллекту?» ИТ-специалист 19, вып. 4 (2017): 7–11. https://doi.org/10.1109/MITP.2017.3051326.

ICO. «Принцип (a): законность, справедливость и прозрачность», 6 ноября 2019 г. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection регулирование-ВВП / принципы / законность-справедливость-и-прозрачность.

Джип ван Левенштейн. «Исключение наблюдения». По состоянию на 14 марта 2020 г. http://www.jipvanleeuwenstein.nl/.

Кикучи, Дайсуке. «Козырек конфиденциальности препятствует технологии распознавания лиц». The Japan Times, 13 мая 2016 г.

https://www.japantimes.co.jp/news/2016/05/13/national/privacy-glasses-thwart-face-recognition-tech/.

Клоско, Георгий. «Принцип справедливости и политических обязательств». Этика 97, вып. 2 (1 января 1987 г.): 353–62. https://doi.org/10.1086/292843.

Крамер, Филипп. 'Искусство. 5 '. В Datenschutz-Grundverordnung. Bundesdatenschutzgesetz Und Nebengesetze. Комментарий, отредактированный Мартином Эссером, Филиппом Крамером и Каем фон Левински, 6-е изд., 2018.

Краненборг, Херке. «Статья 8 - Защита личных данных». В Хартии основных прав ЕС: комментарий, под редакцией Стива Пирса, Тамары Херви, Джеффа Кеннера и Анджелы Уорд, 01 изд., 223–66, 2014.

Куо, Лили. «Новая норма»: чрезмерный общественный мониторинг коронавируса в Китае может сохраниться ». The Guardian, 9 марта 2020 г., сек. Мировые новости. https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

Мальджери, Джанклаудио. «Концепция справедливости в GDPR». Труды FAT * '20, 27–30 января 2020 г., 2020 г. https://doi.org/10.1145/3351095.3372868.

ОЭСР. Руководящие принципы защиты конфиденциальности и трансграничных потоков персональных данных (2013 г.).

Филлипс, Роберт А. «Теория заинтересованных сторон и принцип справедливости». Деловая этика Ежеквартально 7, вып. 1 (январь 1997 г.): 51–66.

https://doi.org/10.2307/3857232.

Ролз, Джон. «Справедливость как честность». Философское обозрение 67, вып. 2 (1958): 164–94. https://doi.org/10.2307/2182612.

Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46 / ЕС (Общие правила защиты данных) (Текст, имеющий отношение к ЕЭЗ), Pub. L. No. OJ L 119, стр. 1–88. По состоянию на 12 августа 2019 г.

https://eur-lex.europa.eu/eli/reg/2016/679/oj?eliuri=eli%3Areg%3A2016%3A679%3Aoj.

Росснагель, Александр. «Артикель 5». В Датеншутцрехте. DSGVO Mit BDSG, под редакцией Спироса Симитиса, Геррита Хорнунга и Индры Шпикер, 363–99. Номос, 2019.

Смит, Аарон. «Более половины взрослых в США доверяют правоохранительным органам ответственно использовать распознавание лиц». Исследовательский центр Pew, nd

https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf.

«Право на неприкосновенность частной жизни в эпоху цифровых технологий. Доклад Верховного комиссара ООН по правам человека ». Совет по правам человека, 2018.

https://daccess-ods.un.org/TMP/1219208.61303806.html.

Ван Бюрен, Гарри Дж. «Если проблема - справедливость, то решение является ли согласие? Интеграция теории истины и заинтересованных сторон». Академия управленческих работ 1999, вып. 1 (1 августа 1999 г.): C1–6.

https://doi.org/10.5465/apbpp.1999.27630644.

Европейская комиссия. «Белая книга по искусственному интеллекту: европейский подход к совершенству и доверию». Текст. По состоянию на 14 марта 2020 г.

https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust

Ограничение целей дизайном как против функциональной ползучести и системной безопасности в police ai

Иво Эмануилов, Стефано Фантин, Томас Маркен, Пликсавра Вогиатцолгу[363]

Двойственная природа ИИ делает его одновременно угрозой и средством защиты прав человека и систем информационных технологий.

Среди прочего, проблемы, касающиеся непрозрачности и включения потенциальных предубеждений в алгоритмические процессы, а также присущие уязвимости таких приложений уязвимости безопасности, выявляют противоречие между такими технологическими ловушками и пригодностью действующей нормативно-правовой базы. Как следствие, нормативные концепции, возможно, придется пересмотреть, чтобы поддержать развитие ИИ.

В этом документе отражается важность принципа ограничения целей и его роль на этапе проектирования для смягчения негативного воздействия ИИ на права человека и безопасность информационных систем.

Определение, разработка и «изготовление» цели, для которой используется ИИ, имеет решающее значение для смягчения вторжения в права человека.

---

[363] Докторанты в Центре права информационных технологий и интеллектуальной собственности KU Leuven. Все авторы в равной степени внесли свой вклад в подготовку и исследование этой статьи.

Однако неизбежная неопределенность в формулировке этих целей может привести к сценариям, в которых машины делают то, что мы просим их делать, но не обязательно то, что мы намерены. Более того, постоянное развитие возможностей системы может позволить использовать ее далеко за пределами ее первоначально предполагаемого развертывания и цели.

В контексте ИИ развертывание ИИ за пределами его первоначально указанных, явных и законных целей может привести к сбою функций, а также к усугублению инцидентов безопасности. Например, системы искусственного интеллекта, предназначенные для конкретных целей предупреждения преступности, могут постепенно перепрофилироваться для необоснованной деятельности по наблюдению, которая изначально не рассматривалась. Кроме того, отсутствие определенной цели в сочетании с присущими технологиям искусственного интеллекта уязвимостями безопасности ставит под сомнение пригодность использования инструментов машинного обучения в сложных системах информационных технологий.

В законе о защите данных принцип ограничения целей требует, чтобы цели, для которых обрабатываются данные, были указаны, а последующее использование ограничено ими (OECD, 1981). В этой статье делается попытка определить, может ли этот принцип устранить последствия сползания функций, исследуя варианты использования прогнозирующего контроля и безопасности информационных систем.

Утверждается, что, хотя этот основной принцип может повысить безопасность систем искусственного интеллекта и их большее соответствие с правами человека, в настоящее время этого часто не происходит. Мы предлагаем провести более точную оценку предполагаемых целей на этапе проектирования, чтобы повысить безопасность систем ИИ и их лучшее соответствие с правами человека.

Ключевые слова: искусственный интеллект, ограничение цели, защита данных, предиктивная полиция, кибербезопасность.

Вступление

Машинный или искусственный интеллект (ИИ) часто определяется как способность машин действовать таким образом, чтобы помогать им в достижении их целей. По сути, эти машины оптимизации включают цели и пожелания, поставленные их разработчиками и пользователями.

Однако со временем ИИ, будь то сама система или ее предполагаемое использование, может превзойти первоначальные цели, предусмотренные в процессе проектирования. В стремлении к оптимизации социальной безопасности несовпадение целей и развертывание ИИ за пределами его первоначально определенных, явных и законных целей может привести к замедлению функционирования, потенциально угрожающему правам человека[364].

Еще в 1960 году Норберт Винер выразил озабоченность по поводу того, что если мы используем для достижения наших целей механическое агентство, в работу которого мы не можем эффективно вмешиваться, нам лучше быть полностью уверенными в том, что цель заложеная в машину – это цель, которую мы действительно желаем»[365]. Таким образом, определение, разработки и «изготовление» цели, для которой используется ИИ, имеет решающее значение для смягчения вторжения в права человека. Однако неизбежная неопределенность в формулировании этих целей может привести к сценариям, в которых машины делают то, что мы просим их делать, но не обязательно то, что мы намереваемся[366]. Более того, непрерывное развитие возможностей системы может позволить использовать их далеко за пределами области применения его первоначально предполагаемого развертывания и цели. Например, системы искусственного интеллекта, предназначенные для конкретных целей предупреждения преступности, могут постепенно перепрофилироваться для необоснованной деятельности по наблюдению, которая изначально не рассматривалась. Кроме того, отсутствие определенной цели в сочетании с присущими ИИ уязвимостями безопасности ставит под сомнение целесообразность использования инструментов, управляемых данными, в сложных системах информационных технологий.

На этом фоне в документе утверждается, что нынешняя интерпретация правового принципа ограничения целей, истоки которого лежат в законе о защите данных, не позволяет устранить риски неблагоприятного воздействия на права человека. Мы предлагаем провести более точную оценку предполагаемых целей на этапе проектирования, чтобы повысить безопасность систем искусственного интеллекта и их лучшее соответствие с правами человека.

---

[364] Такие, как, например, «радикализация» чат-бота Microsoft Tay и неблагоприятные последствия подталкивания алгоритмов выбора контента по клику. Другой пример - неоднозначное использование инструментов оценки рисков в уголовном правосудии, таких как системы профилирования исправительных правонарушителей для альтернативных санкций (COMPAS), используемые в США. См. «Уголовное право - Рекомендации по вынесению приговоров - Верховный суд штата Висконсин требует предупреждения перед использованием алгоритмической оценки риска при вынесении приговора - Государство против Лумиса 881 NW2d 749 (Висконсин, 2016 г.), Недавние дела», Harvard Law Review 130, no. 5 (2016–2017): 1530–37.

[365] Норберт Винер, «Некоторые моральные и технические последствия автоматизации», Наука, 131, вып. 3410 (5 июня 1960 г.): 1358, https://doi.org/10/ftpxdb.

[366] Рассел, Совместимость с людьми, 12.

Статья состоит из трех основных частей. В первом разделе представлен генеалогический обзор принципа ограничения цели в законе о защите данных и предлагается другой подход к смягчению негативного воздействия сползания функций. Во втором и третьем разделах проблема расползания функций анализируется в контексте двух конкретных случаев: прогнозирующая полицейская деятельность и информационная безопасность в правоохранительном секторе.

Функция цели в ИИ

Ползучесть функций в просторечии упоминается как расширение предполагаемого использования технологии для другого использования, влекущее за собой ряд непреднамеренных и неконтролируемых последствий[367]. Недавнее определение, предложенное Купсом, описывает это как «обозначающее незаметно преобразующее и, следовательно, оспариваемое изменение. в надлежащей деятельности системы обработки данных»[368].

В контексте ИИ мы концептуализируем ползучесть функций как относящуюся к трем основным группам случаев. Первый касается проблемы технологии выполнения задач[369]. Например, системе ИИ может быть поставлена конкретная цель для выполнения задачи оптимизации, но способ определения этой цели может запустить процесс оптимизации, который, в конечном итоге, не достигает намеченной цели разработчика системы. Второй относится к проблеме развертывания технологии, предназначенной для конкретной цели, для другого использования или контекста, что может привести к непредвиденным последствиям[370]. Третье касается сценария, в котором пользователь, оснащенный новыми возможностями, переходит к

---

[367] Проблема смещения функций широко изучалась в области исследований в области наблюдения, защиты данных
и законодательства о конфиденциальности. См., В частности, Langdon Winner, Autonomous Technology: Technics-out-of-Control as a Theme в политической мысли (Cambridge, Mass: MIT Press, 1977), 28 и Дэвида Лайона, Surveillance Studies: An Overview (Polity, 2007).),

[368] Берт-Яап Купс, «Концепция ползучести функций», Право, инновации и технологии 13, вып. 1, перед печатью опубликовано 3 марта 2020 г., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903 спроектирован для выполнения, но результат которого не отражает намеченную цель его разработчиков.

[369] Этот случай касается внутренней проблемы с производительностью оптимизации системы. Например, это может быть результатом чрезмерной оптимизации программного обеспечения для распознавания лиц, что привело
к непреднамеренной расовой дискриминации. См. Фумио Шимпо, «Основная японская стратегия искусственного интеллекта и роботов для установления основных принципов», в Справочнике по исследованию закона искусственного интеллекта (Эдвард Элгар Паблишинг, 2018), 116, https://www.elgaronline.com/view/edcoll /9781786439048/9781786439048.00015.xml.

[370] Это касается проблемы, когда лица, принимающие решения, развертывают технологию в сценарии использования, для решения которого она никогда не предназначалась.

использовать технологию для новой цели. Это тот случай, когда цели пользователя переплетаются с целью оптимизации машины. Другими словами, цель системы – максимизировать ожидаемую полезность путем предложения «гипотез о будущем, основанных на всем ее прошлом опыте»[371] подталкивает пользователя к развертыванию технологии для другой цели.

Можно утверждать, что каждая из этих форм перераспределения функций в контексте ИИ может отрицательно повлиять на осуществление и защиту всего спектра прав человека[372]. Чтобы противостоять этим воздействиям, политики обратили внимание на правовые инструменты, главным из которых являются так называемый принцип ограничения цели. Однако его применение на практике было затруднено из-за неуловимости концепции и контекстной зависимости.

В частности, принцип ограничения цели уходит корнями в руководящие принципы организации экономического сотрудничества и развития в отношении конфиденциальности и в Конвенцию 108 и, как считается, включает два суб-принципа: спецификацию цели и принципы ограничения совместимого использования или совместимости[373]. Аналогичным образом предусмотренный в законодательстве ЕС принцип ограничения цели гарантирует, что персональные данные должны обрабатываться для заранее определенных целей и не обрабатываться в дальнейшем способом, несовместимым с этими целями, за исключением исключительных обстоятельств[374]. Принцип, закрепленный в теориях информационного самоопределения, позволяет человеку получить контроль над своими личными данными[375], хотя индивидуальный контроль в

---

[371] Рассел, Совместимость с людьми, 37.

[372] 10 Лорна МакГрегор, Дараг Мюррей и Вивиан Нг, «Международное право в области прав человека как основа для алгоритмической отчетности», Ежеквартальный отчет по международному и сравнительному праву 68, вып. 2 (2019): 315–316.

[373] Руководящие принципы ОЭСР по защите конфиденциальности и трансграничных потоков персональных данных, 1981 г. (обновлено в 2013 г.), статья , https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
(по состоянию на 18 сентября 19) ; Конвенция 108, статья 5.

[374] Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46 / ЕС (Общий регламент по защите данных), (GDPR), OJ L 119, 4.5.2016, 1–88, статья 5.1 (b); Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования преступников. правонарушений или исполнения уголовных наказаний, а также
о свободном перемещении таких данных, а также об отмене Рамочного решения Совета 2008/977 / JHA, OJ L 119, 4.5.2016, p. 89–131 (ДПЛЭД), статья 4.1 (б); Директива 95/46 / ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, OJ L 281, 23.11.1995, p. 31–50 (DPD), статья 6.1 (b).

[375] Лиана Колонна, «Интеллектуальный анализ данных и его парадоксальная связь с принципом ограничения целей»,
в книге «Перезагрузка междисциплинарных взглядов на защиту данных и современные проблемы», ред. Серж Гутвирт, Рональд Линес, Пол Де Херт (Springer, Нидерланды, Дордрехт, 2014), 299.

правоохранительной среде, возможно, оспаривается как нереалистичный[376]. Принцип ограничения цели предлагает сбалансированный подход между разумными ожиданиями физических лиц, повышая доверие и правовую определенность, и определенные конкурирующие интересы, признавая прагматическую необходимость дальнейшей обработки в конкретных случаях[377].

С одной стороны, принцип определения цели фокусируется на четком разграничении целей, для которых изначально собираются личные данные. Принцип совместимости, с другой стороны, направлен на предотвращение дальнейшей обработки персональных данных для целей, несовместимых с целью, для которой данные были первоначально собраны. Совместимость можно оценить с помощью набора факторов, включая связь между целями, контекстом, характером данных, возможными последствиями и наличием гарантий. Исключения из теста на совместимость предусмотрены для защиты [среди прочего] национальной безопасности, общественной безопасности[378] и предотвращения уголовных преступлений[379]. Кроме того, принцип ограничения цели может быть ограничен в целом, поскольку ограничение уважает сущность основных прав и свобод и является необходимой и соразмерной мерой в демократическом обществе для защиты тех же целей[380].

Ограничение цели практически идентично определено как в Общем регламенте защиты данных (GDPR), так и в сопровождающей его Директиве

---

[376] Кэтрин Яссеран, «Последующее использование данных GDPR в правоохранительных целях: забытый принцип ограничения целей», Обзор европейского законодательства о защите данных 4, вып. 2 (2018): 152.

[377] Статья 29 Рабочая группа по защите данных (WP29), «Мнение 03/2013 об ограничении цели», WP 203, 2 апреля 2013 г.

[378] GDPR, статья 6 (4), согласно статье 29 Рабочей группы по защите данных, Заключение 03/2013. Кроме того, дальнейшая обработка в исторических, статистических или научных целях по закону не считается несовместимой
с GDPR, статья 5.1 (b).

[379] GDPR, статья 6 (4). Другими словами, такой закон предусматривает новую правовую основу, делающую оценку совместимости недействительной. Это положение подверглось критике со стороны WP29 и Европейского надзорного органа по защите данных (EDPS) за игнорирование того факта, что создание правовой основы и соблюдение принципа ограничения цели состоят из двух отдельных совокупных требований. Несмотря на то, что соответствующие мнения относились к предлагаемой версии статьи 6 (4) проекта GDPR, эта линия критики все еще остается в силе, поскольку текущая версия, хотя и существенно изменена, имеет более узкий охват, однако полностью не решает поднятую озабоченность. Статья 29 Рабочая группа по защите данных, Заключение 03/2013; Европейский надзорный орган по защите данных (EDPS), «Мнение Европейского надзорного органа по защите данных о пакете реформы защиты данных», Брюссель, 7 марта 2012 г., https://edps.europa.eu/sites/edp/files/publication/12- 03-07_edps_reform_package_en.pdf

[380] GDPR, статья 23. В то время как соответствующее положение об ограничениях в DPD и в проекте GDPR прямо называет принципы качества данных, включая, помимо прочего, принцип ограничения цели, которые должны быть включены в объем ограничения, формулировка окончательного текста предусматривает это отличная и расплывчатая структура. Таким образом, неясно, в какой степени ограничение цели считается соответствующим «правам или обязанностям» или отбрасывается как основополагающий принцип. См. Также Кэтрин Яссеран, Последующее использование данных GDPR в правоохранительных целях: забытый принцип ограничения целей.

(ЕС) 2016/680 (DPLED)[381], которая применяется к обработке персональных данных компетентными органами в целях предотвращения, расследования, раскрытие и преследование преступлений. Тем не менее, совместимость в последнем далее не объясняется, а исключения не сформулированы таким же подробным образом. В частности, DPLED сосредоточен на различии между «целями правоохранительных органов» и «целями, не имеющими отношения к правоохранительным органам», а не на формулировке того, как цели в рамках правоохранительных органов могут быть разными и несовместимыми. С этой целью было указано, что каждая отдельная цель обработки должна быть подробно описана, поскольку «правоохранительные органы как таковые не должны рассматриваться как одна конкретная, явная и законная цель»[382], и две цели правоохранительных органов не должны рассматриваться и фактически считаться совместимыми, потому что они принадлежат к одной области[383]. Однако из-за правовой природы DPLED применение принципа ограничения цели будет колебаться в зависимости от национального имплементирующего законодательства.

Наконец, функция цели в прецедентном праве ЕС в области прав человека также неуловима. В случаях наблюдения Суд ЕС, например, стремится уподобить наличие общей цели обеспечения безопасности наличию цели, представляющей общий интерес,[384] несмотря на закрепление принципа определения цели в Хартии фундаментальных Права ЕС (CFREU) как часть права на защиту данных[385].

Однако такой подход делает принцип ограничения цели, по сути, бесполезным; В соответствии с CFREU проверка наличия цели, представляющей общий интерес, проводилась бы независимо от того, какое право имеет неабсолютное право.

Более того, принцип ограничения цели часто упускается из виду на оперативном уровне без конкретных мер по его обеспечению. Вопреки духу принципа, описанного выше, простое наличие цели правоохранительных органов часто приравнивается к соблюдению принципа ограничения цели. Применяется, казалось бы, более узкий подход, когда каждая отдельная часть

---

[381] 19 GDPR, статья 5.1 (b) и DPLED, статья 4.1 (b).

[382] Статья 29 Рабочая группа по защите данных (WP29), Заключение 03/2015 о проекте директивы о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования уголовных преступлений. или исполнение уголовных наказаний и свободное перемещение таких данных », WP 233, 1 декабря 2015 г.

[383] Заключение Европейского надзорного органа по защите данных (EDPS) о пакете реформы защиты данных, 12 марта 2012 г.

[384] См., Например, Суд Европейского Союза, C-293/12 Digital Rights Ireland, C-203/15 и C-698/15 Tele2 Sverige / Watson, Opinion 1/15, C-207/16 Ministerio Fiscal.

[385] Хартия Европейского Союза об основных правах (CFREU), OJ C 202, 7.6.2016, 391–407, статья 8.

принципа, то есть спецификация цели, совместимость и ее ограничение при условии необходимости и соразмерности, не полностью принимаются во внимание. Отсутствие такой проверки способствует этому незаметному перенацеливанию системы ИИ, что создает пространство для сползания функций.

Мы полагаем, что на этапе проектирования необходимы усилия по интеграции более глубокого анализа ограничений цели[386]. Подход, основанный на разработке, мог бы обеспечить и навязывать осознанную, прозрачную и всестороннюю оценку первоначальной цели, потенциально совместимых дальнейших целей и ограниченного использования для несовместимых целей только в пределах пригодности, отсутствия менее интрузивных альтернативных средств и строгой соразмерности[387]. Таким образом, этот подход позволил бы устранить ползучесть функций и текущие недостатки.

Ограничение цели в контексте правоприменения. Более того, ограничение цели может также служить каналом для лучшего понимания приемлемого уровня развертывания ИИ, сосредоточив внимание на связанных с этим рисках безопасности.

Таким образом, конечные пользователи системы и производители должны вступить в открытый диалог относительно назначения предполагаемых инструментов. Перед развертыванием на уровне программного обеспечения должны быть включены четкие ограничения и ограничения на системные процессы и функции, чтобы предотвратить постепенное использование приложений для различных и более широких целей. В документе будет предпринята попытка лучше проиллюстрировать это через призму методов прогнозирования и уязвимостей информационной системы полиции.

Предиктивная политика

Концепция

В общих чертах, концепция прогнозирующей полицейской деятельности относится к использованию аналитических методов для оценки широкого

---

[386] CFREU, статья 52 (1).

[387] Принцип соразмерности в праве прав человека предполагает, что ограничительная мера должна быть подходящей
и подходящей для достижения цели, наименее обременительной по отношению к этой цели и соразмерной stricto sensu, т. Е. Достижению справедливого баланса. См., Например: Йонас Кристоффersен, Справедливый баланс: соразмерность, субсидиарность и первенство в Европейской конвенции о правах человека (Martinus Nijhoff Publishers, 2009).

спектра данных с целью прогнозирования потенциальных преступлений[388]. Используя статистические модели, инструменты прогнозирующей полицейской деятельности могут наиболее часто определять места, людей и обстоятельства могут быть причастны к преступным действиям[389]. Эта информация может быть использована для руководства действиями полиции и поддержки способности правоохранительных органов оценивать данные о преступности с целью принятия упреждающих и целенаправленных действий.

С этой целью инструменты прогнозирования полиции обычно делятся на две основные категории. Прогнозное картографирование или методы, ориентированные на места, нацелены на то, чтобы предвидеть места, в которых наиболее вероятно совершение преступления в данное время и при определенных обстоятельствах[390]. Эти методы могут определять так называемые «горячие точки» для эффективного развертывания ресурсов полиции путем анализа полицейских досье, тенденций преступности и других переменных, имеющих отношение к совершению преступных действий.

Аналогичным образом, прогнозирующая идентификация или приложения, ориентированные на человека, стремятся определить, какие лица имеют больше шансов совершить преступления или стать жертвой из-за этого[391]. Путем проведения оценки рисков и установления обстоятельств, повышающих вероятность причастности лица к преступлению, правоохранительные органы агентства могут выявлять лиц, относящихся к группе повышенного риска, чтобы активно вмешиваться и уводить их от преступлений.

Помимо использования этих методов правоохранительными органами и государственными органами, прогнозирующая полицейская деятельность может также повлечь за собой участие частных лиц. Например, часть борьбы с финансовой преступностью, отмыванием денег и финансированием терроризма передается на аутсорсинг банкам, которые должны соблюдать свои обязательства перед ЕС по борьбе с отмыванием денег (AML)[392]. Пытаясь

---

[388] Бет Пирсолл, «Предиктивная работа полиции: будущее правоохранительной системы?», Национальный институт юстиции, журнал 266, вып. 1 (2010).

[389] Уолтер Л. Перри, Брайан Макиннис, Картер С. Прайс, Сьюзан С. Смит, Джон С. Голливуд, Предиктивная полицейская деятельность: роль прогнозирования преступности в правоохранительных операциях (RAND Corporation, 2013).

[390] Совещание экспертов PHRP по прогнозируемой деятельности полиции (Международная амнистия, полиция и программа по правам человека, май 2019 г.)

[391] 29 Фике Янсен, Работа полиции на основе данных в контексте Европы (Рабочий документ Data Justice Lab, май 2018 г.).

[392] 30 Директива (ЕС) 2018/843 Европейского парламента и Совета от 30 мая 2018 г. о внесении поправок в Директиву (ЕС) 2015/849 о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма и внесение поправок Директивы 2009/138 / ЕС и 2013/36 / EU, OJ L 156, 19.6.2018, 43–74. Для получения дополнительной информации о политике и законодательстве по противодействию отмыванию денег и финансированию терроризма посетите официальный сайт Европейской комиссии https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision -and-risk-management /

выполнить последнее, банки часто прибегают к прогнозной аналитике транзакционной деятельности, чтобы определить потенциальное преступное поведение в будущем и, если возможно, предотвратить проявление преступности[393]. Однако, в то время как прогнозная аналитика, используемая правоохранительными органами, основывается в основном на криминальных данных, прогнозная аналитика, выполняемая банковским сектором учреждения полагается в первую очередь на данные, полученные в ходе регулярных коммерческих и финансовых операций. Тем не менее, основная логика остается той же, и используемые алгоритмы должны быть обучены для выявления потенциально преступных намерений, стоящих за транзакциями.

Более того, хотя технологии, лежащие в основе прогнозирующей полицейской деятельности, имеют большие перспективы и часто преподносятся как революция в борьбе с преступностью[394], эффективность и влияние этой практики по-прежнему оспариваются. Несмотря на растущее использование инструментов прогнозирования полицейской деятельности во всем мире[395], эмпирические данные еще не окончательно подтвердили утверждения о последовательном и значительном сокращении преступности[396].

Аналогичным образом, часто высказываются серьезные опасения по поводу потенциально негативного воздействия на права человека, и ответственность полиции, и справедливость вмешательства правоохранительных органов[397]. Именно в контексте этого противоречия и неопределенности цель данной статьи – оценить риски нарушения функций в средствах прогнозирования полицейской деятельности, которые могут усугубить эти проблемы и могут потребовать другого подхода к ограничению целей для улучшения подотчетности и надежности этих приложений.

борьбе с отмыванием денег и финансированием терроризма_en.

[393] См., Например, EY Global, «Как анализ данных ведет борьбу с финансовыми преступлениями», EY Global (блог), 6 декабря 2019 г. https://www.ey.com/en_be/advisory/how-data-analytics- ведет борьбу с финансовыми преступлениями.

[394] 32 Джоэл Рубин, «Прекращение преступности до ее начала», Los Angeles Times, 21 августа 2010 г.; Зак Френд, «Предиктивная работа полиции: использование технологий для снижения преступности», Бюллетень правоохранительных органов ФБР, 9 апреля 2012 г.

[395] Одран Джеймс Маккарти, «ИИ и глобальное управление: переломить ситуацию с преступностью с помощью прогнозирующей полицейской деятельности», Статьи и аналитика по ИИ и глобальному управлению (Центр политических исследований Университета ООН, 26 февраля 2019 г.), https: //cpr.unu .edu / ai-global-Governance-Turn the-tide-on-Crime-with-predictive-policing.html.

[396] Альберт Мейер и Мартин Весселс, «Предиктивная полицейская деятельность: обзор преимуществ и недостатков», Международный журнал государственного управления 42, вып. 12 (2019).

[397] Ханна Каучман и Алессандра П. Лемос, Работа полиции с помощью машины: прогнозирование и угроза нашим правам (Liberty Human Rights, 2019).

Ползучесть функции и пределы ограничения цели

Ограничение цели в его нынешнем виде не представляется эффективной защитой в контексте прогнозируемой полицейской деятельности. Поскольку эти приложения постепенно применяются для все более широких целей, а расширяющиеся наборы данных, к которым имеет доступ полиция, используются для любых и всех соответствующих аналитических процессов[398], ограничение цели кажется неспособным устранить риск потери функций. Это связано с широким мандатом правоохранительных органов на борьбу с преступностью, обширными основаниями для сбора и использования личных данных, последующим ростом объемов данных, к которым они могут получить доступ и которые они могут хранить, а также с возможностями больших данных инструментов, которые они используют.[399] Более того, множество факторов, таких как рост террористических угроз и оцифровка преступности, привели к растущему дублированию компетенций правоохранительных и разведывательных служб, что увеличивает объем данных и органов, имеющих доступ к ним[400].

В контексте прогнозной полицейской деятельности это проявление ползучести функций в первую очередь касается риска использования аналитических инструментов для все более широких целей, стирающих границы с практикой массового наблюдения. В то время как ранние итерации инструментов прогнозирования полиции ограничивались внесением скромных улучшений в существующие методы, основанные на разведке, которые позволяли более точно определять области повышенного риска[401], технологических достижений и растущая доступность больших данных позволили прогнозным системам анализировать более крупные наборы данных, учитывать больше переменных и делать все более далеко идущие выводы о местах и людях[402]. Кроме того, порог включения в базы данных правоохранительных органов часто низок, а объем анализируемых данных

---

[398] Сара Брейн, «Наблюдение за большими данными: пример полицейской деятельности», Американский социологический обзор 82, вып. 5, 2017.

[399] Йорис ван Хобокен, «От сбора к использованию в регулировании конфиденциальности? Перспективное сравнение европейских и американских структур для обработки персональных данных », в« Исследование границ больших данных », ред. Барт ван дер Слоот, Деннис Бродерс и Эрик Шрайверс (Научный совет Нидерландов
по государственной политике, 2016).

[400] 38 Джон Верваэле, Наблюдение и уголовное расследование: размывание порогов и границ в системе уголовного правосудия ?; Алесь Заврсник, «Размытие границы между правоохранительными органами и разведкой: усиление наблюдения?» Журнал современных европейских исследований 9, № 1 (2013): 52.

[401] 39 Рутгер Ринкс, Предиктивная работа полиции: шанс на более безопасное будущее (Politieacademie Lectoraat Intelligence, 2015).

[402] Войцех Филипковски, «Предиктивная полицейская деятельность с использованием последних технологических достижений», Презентация ежегодного собрания ASC, Сан-Франциско, 15 ноября 2019 г.

часто расширяется за счет включения внешней информации[403], такой как счета за коммунальные услуги, заказы на доставку и кадры распознавания автомобильных номеров[404]. Таким образом, обширный характер методов прогнозирования полиции создает риск того, что эти инструменты и данные, которые они используют, будут постепенно использоваться и повторно использоваться способами, которые очень похожи на массовое наблюдение, без надлежащих мер предосторожности или заботы. к принципу ограничения цели.

В Соединенных Штатах такие инструменты, как Operation LASER, используются для оценки людей на основе их обстоятельств, личной жизни и взаимодействия с системой уголовного правосудия с целью определения конкретных профилей для дальнейшего наблюдения[405], в то время как программное обеспечение, такое как PredPol, предоставляет карту преступности и прогнозы, чтобы подтолкнуть офицеров к постоянному мониторингу сообществ высокого риска и окрестностей[406]. Аналогичным образом, европейские полицейские агентства, например, в Лондоне[407] и Уэст-Мидлендсе[408] начали развертывание столь же продвинутых программ оценки риска, используемых для выявления лиц и территорий высокого риска, чтобы постоянно отслеживать их вероятность причастности к преступлению на основе обширных наборов данных и широких статистических выводов[409].

Наконец, в случае приватизированной системы прогнозирования полиции, например, когда она используется банковскими учреждениями для предотвращения финансовых преступлений, ограничение цели уже ограничено с момента ее использования. Персональные данные подвергаются дальнейшей обработке с целью предотвращения преступности, которая отличается от исходной и несовместима с исходной, то есть с финансовыми транзакциями. Наличие правовой основы, являющейся обязательствами, не допускает дальнейшего рассмотрения необходимости и соразмерности. Следовательно, любая оценка принципа ограничения цели в этом случае становится устаревшей.

---

[403] 41 Прогностические аналитические инструменты доходят даже до рекламы своих возможностей сочетать полицейские записи с данными из Интернета, информацией из социальных сетей и другими внешними источниками разведывательной информации, касающейся деятельности, истории и местонахождения человека. См., Например, SINTELIX, «Большие данные и аналитика в правоохранительных органах: прогнозирующая политика», SINTELIX (блог), 30 марта 2018 г., https://sintelix.com/blog/big-data-analytics-law-enforcement-полиция /.

[404] Сара Брейн, Наблюдение за большими данными: случай полицейской деятельности.

[405] 43 Крейг Д. Учида и Марк Л. Сватт, «Операция« ЛАЗЕР »и эффективность патрулирования горячих точек: панельный анализ», Police Quarterly 16, no. 3, 2013.

[406] Кристиан Лам и Уильям Исаак, «Предсказывать и служить?», Журнал Significance Journal 10, вып. 5, 2016.

[407] Мэр Лондона, Управление полиции и преступности, Обзор матрицы банд столичной полиции (Отчет, 2018).

[408] Александр Бабута и Марион Освальд, Аналитика данных и алгоритмическая предвзятость в полицейской деятельности (Информационный документ Королевского института объединенных служб, 2019 г.).

[409] Вим Хардинс и Аннелин Рамменс, «Предиктивная работа полиции как новый инструмент для правоохранительных органов?

В свете вышеизложенного, похоже, что принцип ограничения цели в его текущем состоянии не может решить проблему ползучести функций. Однако включение соображений по спецификации цели и совместимости целей уже на этапе проектирования может означать решающий шаг на пути к более эффективному применению принципа и защите систем прогнозируемого контроля от риска нарушения функций. В частности, все вовлеченные стороны, как со стороны разработчиков, так и со стороны правоохранительных органов и разведки, должны будут обсудить прагматические данные, необходимые для систем ИИ, для выявления тенденций преступности и разработки индивидуальных оценок рисков. Это подразумевает лучшее понимание того, как функционирует прогнозная аналитика, и более четкое разграничение типов данных, необходимых для той цели, которую стремится достичь каждая конкретная система ИИ. В зависимости от используемой прогнозной аналитики в систему должны быть встроены ограничения на основе, среди прочего, явных типов данных, происхождения данных, отдельно определенных для преступлений и коммерческих данных, а также типа преступлений, которые система стремится предотвратить. При возникновении вопросов совместимости или необходимости и соразмерности систему можно научить приостанавливать любое действие до тех пор, пока не будет выполнена надлежащая оценка с дополнительными сдержками и противовесами.

Такая практика, прежде всего, повысит предсказуемость и прозрачность прогнозной полицейской аналитики и конкретных целей, для которых она используется. Это еще больше снизило бы риски нарушения функций, не позволяя ни системе AI, ни пользователю расширять объем целей, для которых система используется. Необходимость более глубокого обсуждения того, как применять принцип ограничения целей, до разработки системы искусственного интеллекта с прогнозированием, сделает ее более эффективной и практически осуществимой.

Ограничение цели в обеспечении информационной безопасности

Внедрение ИИ в существующие информационные системы усиливает ландшафт угроз за счет новых уязвимостей безопасности с более высокой степенью неопределенности[410]. В отличие от традиционных уязвимостей

[410] 48 Рик Фергюсон, «Автономное кибероружие - будущее преступности?», Forbes, 10 сентября 2019 г., https://www.forbes.com/sites/rikferguson1/2019/09/10/autonomous-cyber-weapons-the -future-of-Crime / # 36b0ba415b1a; Грег Аллен и Таниэль Чан, Искусственный интеллект и национальная безопасность (Белферский центр науки и международных отношений, Гарвардская школа Кеннеди, 2017) 19 и 26; Майлз Брандейдж и др., Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий (Отчет

кибербезопасности, где недостатки в компьютерных кодах часто являются результатом человеческих ошибок, таких как ошибочное программирование или преднамеренные бэкдоры. Системы искусственного интеллекта включают уязвимости, которые по своей сути зависят от современного состояния технологий[411]. В результате старомодный процесс поиска и исправления может просто не работать, пока технологические исследования не сделают все приложение более эффективными и прочными[412].

Использование прогностических приложений на основе искусственного интеллекта для полицейской деятельности – это тот случай использования, когда надежность и безопасность системы имеют решающее значение для обеспечения соответствия инструмента расследования этическим и фундаментальным правовым принципам[413].

«Последние события и проблемы», Европейский журнал уголовной политики и исследований 24, вып. 3, 2018.

Безопасность системы неразрывно связана с защитой прав личности. По этой причине, а также с учетом экспоненциального расширения ландшафта угроз безопасности, связанных с ИИ, необходимо искать технические и организационные меры для снижения рисков безопасности при развертывании таких технологий[414]. В этом отношении мы считаем, что принцип ограничения цели может быть заимствован из область защиты данных для поддержки принятия процессов оценки рисков информационной безопасности, направленных на отображение – и, таким образом, уменьшение – поверхности атаки. Принятие такого принципа на этапе проектирования требует дальнейшей проработки, чтобы понять, в какой степени такой подход может оказаться жизнеспособным для общей оценки развертывания инструментов прогнозирования.

Среди самых последних нормативных предложений по устранению неопределенностей, связанных с ИИ, повышение прозрачности целей для снижения рисков – это предложение, поддержанное многими авторитетными

о вредоносном искусственном интеллекте, 2018 г.).

[411] Например, как говорит Херпиг: «Уязвимости в обычном программном и аппаратном обеспечении дополняются уязвимостями, специфичными для машинного обучения. Одним из примеров являются данные обучения, которыми злоумышленники могут манипулировать для компрометации модели машинного обучения. Это вектор атаки, которого нет в обычном программном обеспечении, поскольку он не использует обучающие данные для обучения ». Свен Херпиг, Защита искусственного интеллекта (Stiftung Neue Verantwortung, 2019), 2.

[412] Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ в области безопасности и что политики могут с этим сделать (Белферский центр науки и международных отношений, Гарвардская школа Кеннеди, 2019), 3.

[413] См. Европейская комиссия, Об искусственном интеллекте - европейский подход к совершенству и доверию (Белая книга, 19 февраля 2020 г. - COM (2020) 65 final) 10, 18, 21-22. См. Также Рек. 38, 51 и ст. 11, 29 Директивы (ЕС) 2016/680.

[414] См. Майкл Хоровиц и др., Искусственный интеллект и международная безопасность (Центр новой американской безопасности, 2018), 13.

источниками. В 2019 году ОЭСР, цитируя работу Вайнбергера за 2018 год[415], подчеркнула, что одним из способов достижения этой цели является рассмотрение цели использования ИИ с учетом, среди прочего, соображений безопасности: «Для этого потребуется декларация о том, что такое оптимизированная система ИИ, с пониманием того, что оптимизации несовершенны, влекут за собой компромиссы и должны ограничиваться «критическими ограничениями», такими как безопасность и справедливость»[416].

На этом фоне идея обязательного «теста на пригодность» [417] получила определенное внимание. Именно в рамках такого процесса мы видим ограничение цели как поддержку информационной безопасности. Тесты на пригодность можно резюмировать как оценку, которая должна быть проведена до принятия определенной системы искусственного интеллекта, посредством чего участвующих субъектов просят оценить риски безопасности и неопределенности, представленные конкретным развертыванием ИИ. Другими словами, такой подход подразумевает практику, основанную на оценке риска, при которой заинтересованные стороны задают себе вопрос: «Насколько подходит эта система для достижения заявленной цели и как я могу сопоставить эту цель с угрозами безопасности, связанными с внедрением ИИ?». Согласно Comiter, такая оценка должна учитывать пять параметров (добавленная стоимость, легкость атаки, ущерб, альтернативные издержки, альтернативы)[418], и в результате этой проверки должна быть получена задокументированная (таким образом, подотчетная) оценка соответствующего уровня Развертывание ИИ. Это особенно важно, поскольку нарушения безопасности приложений ИИ могут привести к серьезным каскадным эффектам в уже существующих взаимосвязанных информационных системах. При условии, что риски безопасности, связанные с ИИ, часто присущи конкретному использованию, для которого используется ИИ, мы считаем, что понимание параметра ценности (т.е. обоснования социальной выгоды от использования ИИ) может быть улучшено путем внедрения этапа оценки вдохновленный принципом ограничения цели. Это означает, что точная цель, для которой будет развернут ИИ, должна быть объявлена и оценена на этапе проектирования из-за специфики таких рисков, что принесет пользу также для

---

[415] Дэвид Вайнбергер, «Оптимизация вместо объяснения - Максимизация преимуществ машинного обучения без ущерба для его интеллекта», Berkman Klein Center on Medium, 28 января 2018 г.), https://medium.com/berkman-klein-center/optimization-over -explanation-41ecb135763d

[416] Организация экономического сотрудничества и развития (ОЭСР), Искусственный интеллект в обществе (отчет, 11 июня 2019 г.), 93.

[417] Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ и что политики могут с этим сделать, 56.

[418] Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ и что политики могут с этим сделать, 57.

прозрачности постфактум и возможности аудита[419]. Элемент, который следует серьезно учитывать при оценке использования ИИ в контексте правоохранительной деятельности, в результате чего, учитывая асимметричное соотношение сил между гражданами и правительствами, ожидается, что[420] методов расследования будут подвергаться нескольким уровням проверки, включая общественную ответственность, независимый надзор и судебно-медицинская допустимость.

Как мы уже упоминали, такой принцип будет способствовать проверке пригодности только постольку, поскольку он принят и понимается следующим образом. В отличие от закона о защите данных, ограничение цели в рамках теста на соответствие ценности должно учитывать не только (личные) данные, но и всю прогностическую архитектуру. Это связано с внутренними (и неизвестными) рисками безопасности, которые относятся не только к наборам данных.

Таким образом, подход к ограничению целей должен рассматриваться комплексно, то есть с учетом всей инфраструктуры ИИ. Это означает, что нам нужно будет заново смоделировать два основных элемента принципа ограничения цели. Адаптация его к общему подходу к безопасности ИИ-архитектуры в рамках теста на пригодность означала бы переосмысление его основных требований. Спецификация цели будет читаться как система должна быть спроектирована и использоваться для указанного, явного и законного использования, тогда как совместимое использование будет означать, что система должна быть спроектирована таким образом, чтобы она была исключительно совместима с заявленным использованием. Если оценка выявляет несовместимость, то следующим шагом должна быть проведена дальнейшая оценка необходимости и соразмерности развертывания.

Во-вторых, принятие такого принципа в рамках теста на пригодность подразумевает проведение общей оценки, которая оперативно будет происходить на двух разных этапах технологического процесса, жизненного цикла[421]. На этапе открытия это упражнение предполагает тесное сотрудничество между разработчиком ИИ, лицом, принимающим решения, владельцем и конечным пользователем[422], для завершения совместной оценки

---

[419] ОЭСР, Искусственный интеллект в обществе, 95: «При управлении рисками, по-видимому, существует широкое согласие с тем, что« контексты с высокими ставками требуют более высокой степени прозрачности и подотчетности, особенно там, где на карту поставлены жизнь и свобода».

[420] ОЭСР, Искусственный интеллект в обществе, 64.

[421] Комитер пишет: «Необходимо тщательно проанализировать и взвесить последствия [машинного обучения] для безопасности, прежде чем машинное обучение достигнет такой степени внедрения, которая сделает практически невозможным обеспечение апостериорной защиты», Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ в безопасности и что Политики могут с этим справиться.

[422] Обзор ИИ и закупок в правительственных секторах см. В Исследовательской службе Конгресса, Искусственный интеллект и национальная безопасность (отчет, 2019) или в Эндрю Илачински, «ИИ, роботы и рои, проблемы, вопросы и рекомендуемые исследования», (Центр военно-морского анализа 2017).

рисков. В нем цели развертывания ИИ контекстуализируются и оцениваются как с учётом существующих ландшафтов угроз безопасности, так и с учетом новых факторов неопределенности, связанных с таким развертыванием. Использование принципа ограничения цели может быть выполнено гибким или более формальным способом. Последний подход может предполагать превращение ограничения цели (или проверки пригодности) в требование, содержащееся в договорных соглашениях, обязательствах по закупкам, соглашениях об услугах или других нормативных решениях.

На этапе эксплуатации, если владельцу системы потребуется изменить назначение приложения ИИ, необходимо будет снова начать декларацию цели развертывания и противодействие потенциальным угрозам безопасности. Эта оценка должна будет принять во внимание новые риски, которые изменение назначения создает для всей информационной системы. При этом принятие этого принципа в рамках теста на соответствие стоимости означает, что он будет непрерывным упражнением, таким образом охватывая все этапы потенциальной поверхности атаки[423].

Эта рекомендация имеет двойную ценность. С организационной и нормативной точки зрения это сделало бы процесс принятия решений подотчетным и совместным, поскольку он был бы документирован и основан на участии многих заинтересованных сторон. С точки зрения безопасности, развертывание такого обязательного упражнения посредством применения принципа ограничения цели повысит осведомленность всех участников, вовлеченных в процесс, относительно уровня рисков, связанных с доступом к таким приложениям.

Вывод

В этом документе утверждается, что ограничение цели в его текущем приложении может не устранять риски потери функций, возникающие в результате появления систем искусственного интеллекта в области правоохранительной деятельности. Указание законной цели часто сводится к простой ссылке на правовую основу, то есть законы и политические меры по предупреждению преступности, тогда как оценка совместимости, а в случае несовместимости, проверка необходимости и соразмерности, кажется, отсутствует. Всеобъемлющая тенденция к оптимизации всей системы предупреждения преступности с целью смягчения возникающих угроз

[423] Например, среда обучения, среда развертывания, внешний мир. См. Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ в безопасности и что политики могут с этим сделать, 14.

безопасности за счет использования ИИ и прогнозной аналитики отводит ограничению цели второстепенную роль. Это, вероятно, окажет неблагоприятное воздействие на права человека, поскольку риск потери функций грозит постепенным расширением полицейской обработки персональных данных и приводит к практике правоприменения, которая очень похожа на широкое наблюдение без надлежащих гарантий. Таким образом, мы утверждаем, что эффективное соблюдение этого принципа уже на этапе проектирования могло бы защитить права человека от неблагоприятных последствий нарушения функций. Кроме того, альтернативная интерпретация ограничения цели может способствовать лучшей оценке информационной безопасности инструментов искусственного интеллекта, особенно в рамках так называемых тестов пригодности. Чтобы добиться успеха в таком упражнении, мы предлагаем принять ограничение цели на этапе проектирования в качестве инструментальной методологии для уравновешивания законных целей правоохранительных органов с неотъемлемыми рисками информационной безопасности.

Ссылки

Альберт Мейер и Мартин Весселс, «Предиктивная полицейская деятельность: обзор преимуществ и недостатков», Международный журнал государственного управления 42, вып. 12 (2019).

Алесь Заврсник, «Размывание границы между правоохранительными органами и разведкой: усиление наблюдения?» Журнал современных европейских исследований 9, № 1 (2013): 52.

Александр Бабута и Марион Освальд, Аналитика данных и алгоритмическая предвзятость в полицейской деятельности (Информационный документ Королевского института объединенных служб, 2019).

Эндрю Илачинский, «ИИ, роботы и стаи, проблемы, вопросы и рекомендуемые исследования» (Центр военно-морского анализа, 2017 г.).

Статья 29 Рабочая группа по защите данных (WP29), Заключение 03/2015 о проекте директивы о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, выявления или преследования уголовных преступлений или исполнение уголовных наказаний и свободное перемещение таких данных », WP 233, 1 декабря 2015 г.

Статья 29 Рабочая группа по защите данных (WP29), «Мнение 03/2013 об ограничении цели», WP 203, 2 апреля 2013 г.

Берт-Яап Купс, «Концепция ползучести функций», Право, инновации и технологии 13, вып. 1, перед печатью опубликовано 3 марта 2020 г., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547903.

Бет Пирсолл, «Предиктивная работа полиции: будущее правоохранительной системы?», Журнал Национального института юстиции, 266, № 1 (2010).

Кэтрин Яссеран, «Последующее использование данных GDPR в правоохранительных целях: забытый принцип ограничения целей», Обзор европейского законодательства о защите данных 4, вып. 2 (2018): 152.

Хартия Европейского Союза об основных правах (CFREU), OJ C 202, 7.6.2016, 391–407.

Исследовательская служба Конгресса США, искусственный интеллект и национальная безопасность (отчет, 2019).

Совет Европы, Конвенция о защите физических лиц в отношении автоматической обработки персональных данных (Конвенция 108).

Суд Европейского Союза, C-203/15 и C-698/15 Tele2 Sverige / Watson.

Суд Европейского Союза, C-207/16 Ministerio Fiscal.

Суд Европейского Союза, C-293/12 Digital Rights Ireland.

Суд Европейского Союза, Заключение 1/15.

Крейг Д. Учида и Марк Л. Сватт, «Операция« ЛАЗЕР »и эффективность патрулирования горячих точек: панельный анализ», Police Quarterly 16, no. 3, 2013.

«Уголовное право - Руководство по вынесению приговоров - Верховный суд штата Висконсин требует предупреждения перед использованием алгоритмической оценки риска при вынесении приговора - Государство против Лумиса 881 NW2d 749 (Висконсин, 2016 г.), недавние дела», Harvard Law Review 130, no. 5 (2016–2017): 1530–37.

Дэвид Лайон, Исследования слежки: обзор (Polity, 2007), 201.

Дэвид Вайнбергер, «Оптимизация вместо объяснения - максимизация преимуществ машинного обучения без ущерба для его интеллекта», Berkman Klein Center on Medium, 28 января 2018 г.), https://medium.com/berkman-klein-center/optimization-over- объяснение-41ecb135763d.

Директива (ЕС) 2016/680 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных компетентными органами в целях предотвращения, расследования, обнаружения или преследования преступников. правонарушений или исполнения уголовных наказаний, а также о свободном перемещении таких данных и об отмене Рамочного решения Совета 2008/977 / JHA, OJ L 119, 4.5.2016, p. 89–131.

Директива (ЕС) 2018/843 Европейского парламента и Совета от 30 мая 2018 г., вносящая поправки в Директиву (ЕС) 2015/849 о предотвращении использования финансовой системы для целей отмывания денег или финансирования терроризма и изменяющая Директивы 2009/138 / ЕС и 2013/36 / EU, OJ L 156, 19.6.2018, 43–74.

Директива 95/46 / ЕС Европейского парламента и Совета от 24 октября 1995 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, OJ L 281, 23.11.1995, p. 31–50 (DPD)

Европейская комиссия, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en .

Европейская комиссия, Об искусственном интеллекте - европейский подход к совершенству

и доверию (Белая книга, 19 февраля 2020 г. - COM (2020) 65 final) 10, 18, 21-22. См. Также Рек. 38, 51 и ст. 11, 29 Директивы (ЕС) 2016/680.

Заключение Европейского надзорного органа по защите данных (EDPS) о пакете реформы защиты данных, 12 марта 2012 г.

Европейский надзорный орган по защите данных (EDPS), «Мнение Европейского надзорного органа по защите данных о пакете реформы защиты данных», Брюссель, 7 марта 2012 г., https://edps.europa.eu/sites/edp/files/publication/12-03-07_edps_reform_package_en.pdf.

EY Global, «Как аналитика данных ведет борьбу с финансовой преступностью», EY Global (блог), 6 декабря 2019 г. https://www.ey.com/en_be/advisory/how-data-analytics-is-leading- борьба с финансовым преступлением.

Фике Янсен, Работа полиции на основе данных в контексте Европы (Рабочий доклад Data Justice Lab, май 2018 г.).

Фумио Шимпо, «Основная японская стратегия искусственного интеллекта и роботов для установления базовых принципов», в Справочнике по исследованию закона искусственного интеллекта (Edward Elgar Publishing, 2018), 116, https://www.elgaronline.com/view/edcoll/ 9781786439048 / 9781786439048.00015.xml.

Грег Аллен и Таниэль Чан, Искусственный интеллект и национальная безопасность (Белферский центр науки и международных отношений, Гарвардская школа Кеннеди, 2017).

Ханна Каучман и Алессандра П. Лемос, Работа полиции с помощью машины: прогнозирование и угроза нашим правам (Liberty Human Rights, 2019).

Джоэл Рубин, «Прекращение преступности до ее начала», Los Angeles Times, 21 августа 2010 г.

Джон Вервель, Наблюдение и уголовное расследование: размытие порогов и границ в системе уголовного правосудия ?.

Йонас Кристоффersен, Справедливый баланс: пропорциональность, субсидиарность и первичность в Европейской конвенции о правах человека (Martinus Nijhoff Publishers, 2009).

Йорис ван Хобокен, «От коллекции до использования в регулировании конфиденциальности? Перспективное сравнение европейских и американских структур для обработки персональных данных », в книге« Исследование границ больших данных », ред. Барт ван дер Слоот, Деннис Бродерс и Эрик Шрайверс (Научный совет Нидерландов по государственной политике, 2016).

Кристиан Лам и Уильям Исаак, «Предсказывать и служить?», Журнал Significance Journal 10, вып. 5, 2016.

Лэнгдон Виннер, Автономные технологии: неконтролируемая техника как тема политической мысли (Кембридж, Массачусетс: MIT Press, 1977), 28.

Лиана Колонна, «Интеллектуальный анализ данных и его парадоксальная связь с принципом ограничения целей», в книге «Перезагрузка мультидисциплинарных взглядов и современных проблем защиты данных», ред. Серж Гутвирт, Рональд Линес, Пол Де Херт (Springer, Нидерланды, Дордрехт, 2014), 299.

Лорна МакГрегор, Дараг Мюррей и Вивиан Нг, «Международное право в области прав человека как основа для алгоритмической ответственности», Ежеквартальный отчет по международному и сравнительному праву 68, вып. 2 (2019): 315–316.

Маркус Комитер, Атака на искусственный интеллект: уязвимость ИИ в области безопасности и что политики могут с этим сделать (Центр науки и международных отношений Белфера, Гарвардская школа Кеннеди, 2019).

Мэр Лондона, Управление полиции и преступности, Обзор матрицы банд столичной полиции (Отчет, 2018).

Майкл Хоровиц и др., Искусственный интеллект и международная безопасность (Центр новой американской безопасности, 2018).

Майлз Брандейдж и др., Злонамеренное использование искусственного интеллекта: прогнозирование, предотвращение и смягчение последствий (Отчет о вредоносном искусственном интеллекте, 2018 г.).

Норберт Винер, «Некоторые моральные и технические последствия автоматизации», Наука, 131, вып. 3410 (5 июня 1960 г.): 1358, https://doi.org/10/ftpxdb.

Одран Джеймс Маккарти, «Искусственный интеллект и глобальное управление: переломить ситуацию с преступностью с помощью прогнозирующей полицейской деятельности», Статьи и аналитика по ИИ и глобальному управлению (Центр политических исследований Университета Организации Объединенных Наций, 26 февраля 2019 г.), https: //cpr.unu. edu / ai-global-management-turn-the-tide-on-Crime-with-predictive-policing.html.

Руководящие принципы ОЭСР по защите конфиденциальности и трансграничным потокам персональных данных, 1981 г. (обновлено в 2013 г.), https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Организация экономического сотрудничества и развития (ОЭСР), Искусственный интеллект в обществе (отчет, 11 июня 2019 г.).

Совещание экспертов PHRP по прогнозирующей деятельности полиции (Международная амнистия, полиция и программа по правам человека, май 2019 г.).

Последние события и проблемы », Европейский журнал уголовной политики и исследований 24, вып. 3, 2018.

Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46 / ЕС (Общие правила защиты данных), (GDPR), OJ L 119, 4.5.2016, 1–88.

Рик Фергюсон, «Автономное кибероружие - будущее преступности?», Forbes, 10 сентября 2019 г.,

https://www.forbes.com/sites/rikferguson1/2019/09/10/autonomous-cyber-weapons-the- будущее преступности / # 36b0ba415b1a.

Рутгер Ринкс, Предиктивная работа полиции: шанс на более безопасное будущее (Politieacademie Lectoraat Intelligence, 2015).

Сара Брейн, «Наблюдение за большими данными: случай полицейской деятельности», Американский социологический обзор 82, вып. 5, 2017.

СИНТЕЛИКС, «Большие данные и аналитика в правоохранительных органах: прогнозирующая политика», СИНТЕЛИКС (блог), 30 марта 2018 г., https://sintelix.com/blog/big-data-analytics-law-enforcement-policing/.

Стюарт Рассел, Совместимость с людьми: искусственный интеллект и проблема контроля (Penguin Publishing Group, 2019).

Свен Херпиг, Защита искусственного интеллекта (Stiftung Neue Verantwortung, 2019).

Уолтер Л. Перри, Брайан Макиннис, Картер С. Прайс, Сьюзан С. Смит, Джон С. Голливуд, Предиктивная полицейская деятельность: роль прогнозирования преступности в правоохранительных операциях (RAND Corporation, 2013).

Вим Хардинс и Аннелин Рамменс, «Предиктивная работа полиции как новый инструмент правоохранительной деятельности?

Войцех Филипковски, «Предиктивная полицейская работа с использованием последних технологических достижений», Презентация ежегодного собрания ASC, Сан-Франциско, 15 ноября 2019 г.

Зак Френд, «Предиктивная работа полиции: использование технологий для сокращения преступности», Бюллетень правоохранительных органов ФБР, 9 апреля 2012

От доказательств к доказательствам: анализ социальных сетей в уголовных судах италии

Доктор Роберто Мусотто *

Анализ социальных сетей изменил взгляды ученых и аналитиков на человеческие отношения, а также помог понять, почему, когда и как делается конкретный поведенческий выбор и возникающие в результате юридически значимые взаимодействия. Юридические документы, такие как законы, правила и судебные дела, все чаще используются в качестве отправной точки для такого анализа, однако его практическое применение в судебной процедуре скудно

или вообще отсутствует. В связи с этим возникают следующие вопросы: можноли использовать анализ социальных сетей в качестве следственного и судебного инструмента для получения доказательств в суде? Что еще более важно, как он будет помогать прокурорам, судьям, присяжным и защитникам в представлении доказательств во время судебного разбирательства? Каким образом анализ сети может способствовать созданию юридического доказательства?

В этой статье представлены аргументы для понимания того, как такая реализация возможна, и ответов на поставленные выше вопросы. Есть возможности, но также и потенциальные подводные камни для внедрения сетевого анализа как средства создания доказательств. В статье будет использоваться контекст итальянских уголовных судов и его уголовно-процессуального законодательства, чтобы понять, как анализ социальных сетей будет подходить и вести себя, особенно при расследовании серьезных преступлений.

Анализ социальных сетей в уголовных судах может быть успешно использован не только как инструмент расследования, но и как фильтр сокращения затрат на предварительных слушаниях и как эффективный порог для вынесения приговора, позволяющий судьям, обвинению и защите давать и оценивать доказательства. Однако эти преимущества по-прежнему представляют собой потенциальную предвзятость, такую как пределы преступной сети и субъективный способ построения сети.

Ключевые слова: анализ социальных сетей, уголовный процесс, судопроизводство, доказательства, доказательства, уголовное правосудие.

Вступление

Анализ социальных сетей (SNA) – это обширный подход к методологическим методам, который позволяет аналитикам и исследователям исследовать сегменты повторяющихся шаблонов, формирующихся в социальных взаимодействиях[424]. Эти шаблоны, которые формируются между отдельными людьми и между группами, способствуют объяснению решений и вариантов выбора, принимаемых участниками в своей повседневной жизни, потому что их рациональные действия следуют потоку влияний, движимых потребностью максимизировать богатство, полезность или счастье. Решения и взаимодействия могут поощряться или ограничиваться применением закона. Контракт, например, способствует взаимодействию сторон с конкурирующими интересами, а уголовный закон, основной целью которого является сдерживание, может предотвратить такое же взаимодействие. Уголовное право направлено на то, чтобы воспрепятствовать членам общества совершать определенные действия, которые считаются незаконными в соответствии с уголовным законодательством их страны. В случае совершения таких действий уголовно-процессуальное законодательство обеспечивает справедливость, эффективность и результативность всего процесса, гарантируя, что с практической точки зрения, если преступление было совершено, судебный орган вынесет решение.

Актуальность СНС была установлена в течение длительного времени[425] в социальных науках и, в частности, в контексте криминологии, главным образом для описания топологии сети[426] или дифференциальных характеристик,

---

[424] Автор благодарит Ханну Альстрём, Адама Харди, Александру Ирназаров, Ребекку Марплс, Коринн Макэлари, Мартина Нёклеберга, Брайана Нуссбаума, Эстер Парканьи, Янну Пападодимитраки, Марию Грацию Порседду, Камило Дэвид Кенберг и Уоллберг за их комментарии. и предложения. Первая версия этой статьи была представлена на 2-м Ежегодном семинаре по методам права и социальных наук в Университете Осло, Норвегия, в октябре 2018 года. Интервью проводились на мероприятиях, проводимых в соответствии с Правилом Chatham House. Работа была поддержана Исследовательским центром кибербезопасности Limited, деятельность которого частично финансируется Программой совместных исследовательских центров правительства Австралии.

* Центр совместных исследований кибербезопасности, Школа бизнеса и права, Университет Эдит Коуэн, Перт, Австралия. Эл. адрес: r.musotto@ecu.edu.au

Малкольм К. Спарроу, «Применение сетевого анализа к криминальной разведке: оценка перспектив». Соцсети 13, нет. 3 (1991): 251-274. https://doi.org/10.1016/0378-8733(91)90008-H.

[425] Исследования Морено, посвященные заключенным из тюрьмы Синг-Синг и реформаторской школы Гудзона, являются первыми примерами анализа социального взаимодействия между заключенными и преступным поведением см. Джейкоб Л. Морено, Применение группового метода к классификации. Нью-Йорк: Национальный комитет по тюрьмам и тюремному труду, 1932 год; Джейкоб Л. Морено, первая книга по групповой психотерапии. Монографии по психодраме и групповой психотерапии 1, (Beacon House, 1957). Полный обзор криминологических теорий и их взаимодействия с общественными отношениями см. В Alex R. Piquero, ed. Справочник по криминологической теории (John Wiley & Sons, 2015).

[426] То есть расположение сети: Лоуренс М. Бесоу и др., «Графическое отображение топологии сети». Патент США 5 276 789, поданный 14 мая 1990 г. и выданный 4 января 1994 г .; Георги Косинец и Дункан Дж. Уоттс, «Эмпирический анализ развивающейся социальной сети». Наука 311, вып. 5757 (2006): 88-90. И как его форма изменяется при различных ограничениях: Расмус Петерсен Розенквист, Кристофер Дж. Родс и Уффе Кок Виль,

которыми обладает группа, и влияния группы на индивидуальный выбор[427]. В этом контексте академические исследования изучали социальные взаимодействия между людьми, совершающими преступные действия, с точки зрения сетевого сообщества[428].

Несмотря на то, что эти взаимодействия были предметом научных исследований, практическому и процессуальному применению этих методов в судах вообще не уделялось внимания. В этой статье показано, как и где методы анализа социальных сетей могут быть успешно переданы в суды. Судебные документы обычно используются в качестве отправной точки для анализа СНС, что оказывается полезным для понимания того, как работают сети, но субъекты, участвующие в производстве юридических и судебных документов, редко, если вообще когда-либо, используют такую методологию для проведения своих расследований[429].

Причинами этого могут быть: а) нехватка времени на следствие и суд; б) проблемы с управлением затратами на исследование; в) недостаток навыков и знаний, необходимых для проведения такого анализа. В этой исследовательской статье судебные документы рассматриваются как конечная точка анализа, проводимого через социальные сети[430]. В ней рассматривается проблема передачи методов анализа социальных сетей в судебные суды и то, как это можно сделать на практике в контексте уголовно-процессуального законодательства Италии. В этой статье указывается, что анализ социальных сетей может применяться не только в качестве инструмента расследования, но и, несмотря на его потенциальную предвзятость, быть помощником при создании и оценке доказательств на предварительных слушаниях, судебных процессах и вынесении приговора.

Как тематическое исследование отдельной страны, его результаты могут быть обобщены для большинства правовых систем гражданского права, за исключением стран, которые принимают чисто следственную правовую систему[431]. Оно направлено на изменение направления некоторых текущих

«Удаление узлов в криминальных сетях». В 2011 г. Европейская конференция по разведке и информатике безопасности, под ред. Персонал IEEE, 360-365. IEEE, (2011).

[427] Джон Скотт и Питер Дж. Кэррингтон, Справочник SAGE по анализу социальных сетей (Лондон: SAGE, 2011), гл. 17, 236-255, https://methods-sagepub-com.ezproxy.ecu.edu.au/book/the-sage-handbook-of-social-network-analysis.

[428] Йонг Лу и др., «Анализ социальных сетей преступного хакерского сообщества». Журнал компьютерных информационных систем 51, вып. 2 (2010): 31-41.

[429] Автор, интервью с прокурором Нидерландов, сентябрь 2018 г.

[430] Де-факто он нацелен на изменение направления современной литературы о криминальных сетях: от анализа ex post к анализу ex ante.

[431] 8 Необходимо делать различия для тех стран, которые принимают состязательные системы разрешения споров (где применяются те же соображения) и системы следственного общего права (где результаты этой статьи могут не применяться), с точки зрения разнообразия стандартов, необходимых для преобразования собранных доказательств. из расследования или во время судебного разбирательства в судебное доказательство. В следственных правовых системах суд расследует дело и собирает доказательства, которые затем представляются в суде обвиняемому. Следовательно, хотя СНС по-прежнему будет полезным

исследований в анализе социальных сетей и криминологии: многие исследователи изучают, как можно использовать судебные документы для их анализа[432], чтобы предсказать или предотвратить нежелательное поведение. В то время как аналитики и ученые начинают свои исследования с судебного документа[433], в этой статье утверждается, что практикующим юристам будет полезен такой анализ для создания юридически значимого документа.

В идеале эта статья расширяет понятие «судьи-роботы» [434]или «судьи ИИ» [435] в сферу других профессиональных юристов, участвующих в судебных процессах и разрешении споров. Преимущество использования методов анализа социальных сетей внутри судебной системы состоит в том, что они позволяют оценить, являются ли поведение и закономерности, вытекающие из СНС, юридически значимыми или, возможно, нет. В гражданском секторе нейронные сети[436] уже были исследованы при альтернативном разрешении споров в строительных претензиях и были внедрены в некоторых юрисдикциях[437] для небольших автомобильных претензий. Эти два типа исков имеют некоторое сходство и склонны к более автоматизированному процессу, потому что: а) иски однородны (т.е. направлены на получение одинакового эффекта); б) существует ограниченное ;количество аргументов, которые могут

инструментом для расследования, она может не понадобиться на предварительных слушаниях, поскольку отбор и оценка доказательств произошли бы на более ранней стадии без участия защиты. Тематическое исследование данной статьи отражает опыт состязательной системы уголовного права.

[432] Лесли Болл, «Автоматизация анализа социальных сетей: мощный инструмент борьбы с терроризмом». Журнал безопасности 29, вып. 2 (2016): 147–168; Бьюнгун Юн и Ёнтэ Пак, «Патентная сеть на основе интеллектуального анализа текста: аналитический инструмент для тенденций в области высоких технологий». Журнал исследований в области управления высокими технологиями 15, вып. 1 (2004): 37-50.

[433] Лесли Болл, «Автоматизация анализа социальных сетей: мощный инструмент борьбы с терроризмом». Журнал безопасности 29, вып. 2 (2016): 147–168; Пёнгун Юн и Пак Ёнтэ. «Патентная сеть на основе интеллектуального анализа текста: аналитический инструмент для выявления тенденций в области высоких технологий». Журнал исследований в области управления высокими технологиями 15, вып. 1 (2004): 37-50. Посмотрите, среди прочего, как была построена криминальная сеть у Берлускони и др. (2016), Ficarra et al (2019) и Lu et al. (2010): сначала были получены различные судебные документы, а затем закодированы, чтобы сделать предположения о группе. Джулия Берлускони и др., «Предсказание связей в криминальных сетях: инструмент для анализа криминальной разведки». PloS one 11, no. 4 (2016 г.), DOI: https://doi.org/10.1371/journal.pone.0154244; Аннамария Фикара и др., «Анализ социальных сетей взаимосвязей сицилийской мафии». Международная конференция по сложным сетям и их приложениям 8. Анализ социальных сетей взаимосвязей сицилийской мафии, (Springer, Cham, 2019), 440-450; Йонг Лу и др., «Анализ социальных сетей преступного хакерского сообщества». Журнал компьютерных информационных систем 51, вып. 2 (2010): 31-41.

[434] Авива Руткин, «Судья - робот». New Scientist 222, вып. 2973 (2014): 24.

[435] 12 судей с искусственным интеллектом - это те, кому технологии помогают в принятии решений. Робот-судья - это компьютер, который рисует модели и принимает решения без участия человека (Sourdin, 2018). Таня Сурдин, «Судья против робота: искусственный интеллект и принятие судебных решений». UNSWLJ The 41, no. 4 (2018): 1114.

[436] Чафалкар Н.Б., Саяли С. Сандбхор, «Применение нейронных сетей в разрешении споров по поводу эскалации с использованием нейрорешения». KSCE Журнал гражданского строительства 19, вып. 1 (2015): 10-16.

[437] В Великобритании был создан чат-бот для оспаривания штрафов за парковку (Laurie and Potton, 2017). Лори Поинтс и Эд Поттон, «Искусственный интеллект и автоматизация в Великобритании». Информационный документ: 8152 (2017); в то время как Эстония создает «судью AI» для мелких претензий (Fabian, 2020). Седа Фабиан, «Искусственный интеллект и закон: будут ли судьи работать на перфокартах». Общий L. Rev.16 (2020): 4

быть представлены в суде как защита; c) меньший риск неправомерных действий со стороны судов; d) стороны заинтересованы в быстром разрешении иска.

В судах внедрение сетевого анализа в основном направлено на выявление нюансов в судебных делах, а не на преодоление роли и функции юристов по разрешению споров[438].

Будут рассмотрены два насущных вопроса: во-первых, как анализ социальных сетей может занять свое место в правовой системе, и, во-вторых, как он может способствовать доказыванию связей и связей вне всяких разумных сомнений, превращая их из следственных доказательств в судебные доказательства.

Внедрение методов СНС в судебном контексте дает возможность сэкономить время, поскольку анализ закономерностей может быть частично автоматизирован, что облегчает работу судебного преследования. Экономия времени, как следствие, снизит затраты, необходимые для облегчения расследования, судебного преследования и судебного разбирательства, поскольку это сделает всю систему более эффективной. Однако, чтобы воспользоваться этими преимуществами, нынешний недостаток знаний юристов в этой области должен быть преодолен с помощью образования, позволяющего практикующим специалистам понимать как положительные элементы, так и потенциальные ловушки.

Эта статья структурирована следующим образом. В следующем разделе рассматривается сложность анализа социальных сетей при исследовании преступности. В третьем разделе представлена структура уголовно-правовой системы итальянских судов, после чего дается описание возможных интерполяций сетевых методов в соответствии с действующим уголовно-процессуальным кодексом и системой. В четвертом разделе рассматривается и обсуждается значение этих результатов.

Анализ социальных сетей в преступности и юридических исследованиях

На основании судебных документов и юридических источников было проведено несколько исследований с целью применения методов социальных сетей для картирования, описания и даже прогнозирования преступных сетей и поведения сообщества[439]. В таком контексте сообщество не является суммой

---

[438] Также необходимо поднять важные вопросы о правах, о которых идет речь, как описано ниже.

[439] Воробей, «анализ криминальной разведки». 251-274; Мангай Натараджан, «Понимание структуры крупной сети распространения героина: количественный анализ качественных данных». Журнал количественной

независимых решений, сделанных группой индивидуумов, но, как следствие Зиммеля[440], именно результат их взаимодействия постоянно влияет и формирует отношения. В криминальных сетях есть часть сообщества, в которой большинство выступает за тех, кто желает нарушить правила, а не за тех, кто их уважает[441]. Интенсивность и частота этих отношений порождают преступное поведение, что заметно через динамику, которая может проявиться в ходе расследования или судебного разбирательства, поскольку действия людей фиксируются в определенном контексте[442] и временных рамках.

SNA в своей простейшей форме, анализ ссылок[443], уже используется в качестве вспомогательного средства в расследованиях и судебных процессах, особенно в делах об отмывании денег[444] и делах о преступных группировках[445]. Например, в США программное обеспечение COPLINK[446] действует как система баз данных, где различные сущности могут быть связаны через результаты анализа текста. COPLINK обеспечивает анализ ссылок, который в настоящее время проходит испытания[447]. Это более мягкая версия SNA, которая в основном используется в качестве инструмента визуализации. Однако чего по-прежнему не хватает, так это более сложной версии CHC, которая предоставляет поддающиеся измерению доказательства причастности каждого человека или стандарты, установленные преступным поведением.

Кроме того, судебные документы являются одним из различных ресурсов для выявления и построения социальных сетей. Кампана и Варезе (2012)[448],

---

криминологии 22, вып. 2 (2006): 171–192; Эдвард Р. Климанс и Кристиан Дж. Де Пут, «Криминальные карьеры в организованной преступности и структура социальных возможностей». Европейский журнал криминологии 5, вып. 1 (2008): 69-98; Франческо Кальдерони, «Структура мафии наркобизнеса:« Ндрангета и кокаин». Преступность, закон и социальные изменения 58, вып. 3 (2012): 321-349; Морселли, Карло, 2009. Внутри преступных сетей 8 (Нью-Йорк: Спрингер, 2009); Дэвид А. Брайт, Кейтлин Э. Хьюз и Дженни Чалмерс, «Освещение темных сетей: анализ социальных сетей австралийского синдиката незаконного оборота наркотиков». Преступность, закон и социальные изменения 57, вып. 2 (2012): 151–176; Роберто Мусотто, «Социальный и пространственный сетевой анализ организованной преступности». Докторская диссертация, Università degli Studi di Messina (2016).

[440] 17 Георг Зиммель, «Проблема социологии». Американский журнал социологии 15, вып. 3 (1909): 289-320

[441] Эдвин Х. Сазерленд, Дональд Р. Кресси и Дэвид Ф. Лакенбилл, Принципы криминологии (Lanham: AltaMira Press, 1992).

[442] Георги Косинец, «Последствия отсутствия данных в социальных сетях». Социальные сети 28, №1. 3 (2006): 247-268.

[443] Где разные объекты связаны и оцениваются в сети в соответствии с одним из их свойств.

[444] Андреа Ф. Колладон и Элиза Ремонди, «Использование анализа социальных сетей для предотвращения отмывания денег». Экспертные системы с приложениями 67 (2017): 49-58

[445] Дэвис, Роджер Х. «Анализ социальных сетей: помощь в расследовании заговоров». ФБР L. Enforcement Bull 50, (1981): 11; Пол АС. Duijn и Питер РНМ. Клеркс, «Анализ социальных сетей применительно к криминальным сетям: последние события в правоохранительной сфере Нидерландов». В Сети и сетевой анализ для защиты и безопасности, (2014): 121-159.

[446] Дженнифер Шредер, Департамент полиции Тусона, Соединенные Штаты Америки. «COPLINK: интеграция базы данных и доступ к интранету правоохранительных органов, окончательный отчет». Вашингтон, округ Колумбия: Министерство юстиции США (2001).

[447] Пол Джен-Хва Ху и др., «Принятие сотрудниками правоохранительных органов передовых технологий электронного правительства: обзорное исследование COPLINK Mobile». Исследования и приложения электронной торговли 10, вып. 1 (2011): 6-16.

[448] Паоло Кампана и Федерико Варезе, «Прослушивание проводов: критерии и методы количественного анализа

среди других, соглашаются с тем, что доступ к такого рода документам позволяет исследователям собирать данные с прослушивания телефонных разговоров и расследований с определенной степенью достоверности и надежности при условии, что: а) внутри нет самоцензуры; б) широкое групповое покрытие; в) большая выборка разговоров. Применение СНС к тем же юридическим документам, которые используются юридическими операторами, поможет лучше понять исследуемую групповую динамику. С другой стороны, существуют методологические проблемы, касающиеся ограничений сети[449] и проблемы отсутствия информации в скрытых сетях[450], которые выражаются в неясной или неточной динамике внутри группы[451], поскольку расследование могло быть сосредоточено только на одной части сети. всей сети[452] или установить слишком высокий или слишком низкий порог для измерения причастности отдельного лица к незаконной группе.

В более широком контексте следует рассмотреть вопрос о том, почему динамика сети, взятая из этих ресурсов, не может быть более точной: это потому, что существует компромисс между правами людей[453] и необходимостью проведения тщательных расследований и судебных разбирательств. С одной стороны, есть интерес со стороны государства наказывать (ius puniendi)[454] виновного в преступлении и, с другой стороны, право на уважение частной жизни без вмешательства со стороны государственных властей[455]. Благодаря тщательному сочетанию этих двух принципов [456] можно достичь взаимопонимания. сети, избегая при этом ненужного ограничения прав без уважительной причины. В следующем разделе представлено тематическое исследование, описывающее систему уголовного правосудия в Италии, и обсуждается, где сетевые методы могут сосуществовать в рамках этой правовой базы.

перехвата телефонных разговоров». Тенденции в организованной преступности 15, вып. 1 (2012): 13-30.

[449] Т.е. кто может быть частью сети.

[450] Джулия Берлускони, «Все ли имеют значение? Оценка надежности источников данных правоохранительных органов для сетевого анализа прослушиваний ». Global Crime 14, № 1 (2013): 61-81; Антонио Скальоне, мафиозный рети. Cosa Nostra e Camorra: преступные организации противостоят. Франко Анджели, 2011.

[451] Валдис Э. Кребс, «Картографирование сетей террористических ячеек». Подключения 24, нет. 3 (2002): 43-52.

[452] Рене К. Ван дер Хюлст, «Введение в анализ социальных сетей (SNA) как инструмент расследования». Тенденции организованной преступности 12, вып. 2 (2009): 101-121.

[453] Особенно права человека.

[454] Согласно Кельзену (1967), это сила государства, и, таким образом, действуя в интересах субъективных прав других людей, оно выражает и определяет диапазон разрешенного поведения. Ганс Кельсен, Чистая теория права. Беркли: Калифорнийский университет Press, 1967.

[455] Это право, которое присутствует во многих конституциях и конвенциях в разных формулировках. В частности, статья 8, второй раздел Европейской конвенции о правах человека (ЕКПЧ), гласит: «Не должно быть никакого вмешательства со стороны государственных органов в осуществление этого права, кроме случаев, когда это предусмотрено законом и необходимо в демократическое общество в интересах национальной безопасности, общественной безопасности или экономического благополучия страны, для предотвращения беспорядков или преступлений, для защиты здоровья или нравственности или для защиты прав и свобод других.»

[456] Чье обсуждение выходит за рамки данной статьи.

Сетевой анализ и итальянская система уголовного правосудия

Уголовное правосудие Италии – это состязательная система судебного разбирательства[457], в которой прокурор (Pubblico Ministero) и обвиняемый собирают и представляют судье доказательства, которые решают, какие из них могут быть использованы в качестве доказательства при вынесении приговора по предполагаемому преступлению. Процедура[458] – в ее обычной структуре – делится на четыре отдельных этапа: расследование, предварительное слушание, судебное разбирательство и исполнение.

В ходе расследования полицейские, расследующие преступление, собирают косвенные улики. Все доказательства собираются в соответствии с определенной процедурой, которая указана в Уголовно-процессуальном кодексе[459], но могут использоваться и другие методы, если это прямо санкционировано прокурором[460]. По окончании расследования [461] прокурор, если предполагается о совершении преступления, просит полицию арестовать всех лиц, в отношении которых ведется расследование[462]. Мотивация и доказательства собраны в ордере на арест[463].

Есть несколько причин, по которым полезно использовать сетевой анализ в ордере на арест; не только для исследователей, но и для юридических лиц,

---

[457] До 1988 года это была смешанная следственная система, в которой полиции и следственным судьям были предоставлены широкие полномочия по сбору доказательств для передачи в суд (Garofoli, 2008). Винченцо Гарофоли, Diritto processuale penale. (Джуффре Эдиторе, 2008).

[458] В зависимости от конкретного расследуемого преступления и характера исследуемых лиц существуют более сложные или сокращенные процедуры.

[459] Это, в частности, проверка, установление фактов, изъятие улик и прослушивание телефонных разговоров. Прослушивания наиболее важны для построения и исследования сети. Однако все они, а также способ сбора доказательств (например, получение списка контактов или повестки дня) могут способствовать анализу конкретной группы. Например, в судебных процессах сицилийской мафии использование бумажных документов (называемых pizzini) было чрезвычайно полезным для налаживания связей и транзакций между различными аффилированными членами и их жертвами (Musotto, 2016). Роберто Мусотто, «Социальный и пространственный сетевой анализ организованной преступности». Кандидатская диссертация, Università degli Studi di Messina, (2016).

[460] Со временем Верховный суд разрешил использование более сложных инструментов расследования, таких как использование трояна (Cass. N. 26889, 28 апреля 2016 г.) и шпионского ПО (по закону, на этот раз: n. 103/2017). Их использование должно быть оправдано тяжестью и характером расследуемого преступления. Таким образом, он был разрешен для судебных процессов, связанных с мафией и торговлей людьми, но отказался от уголовных преступлений.

[461] Что может длиться максимум до двух лет по особо сложным делам (ст. 407 УПК.)

[462] Согласно Уголовно-процессуальному кодексу Италии, существует разница между арестом и заключением под стражу, которая выделена здесь для ясности. Во-первых, это способность гарантировать преступникам правосудие и не допускать их совершения новых противоправных действий. Он может быть казнен только в том случае, если преступление совершено на месте преступления (преступление совершает лицо) или почти на месте преступления (лицо только что совершило преступление). Он оформляется полицией или, иногда, частными лицами и не может быть выдан. Второй - превентивное задержание, которое применяется во всех других ситуациях, не допускающих арест, и выдается Pubblico Ministero (Государственным прокурором).

[463] Provvedimento di fermo на итальянском языке.

поскольку: 1) это документ, который завершает расследование, поэтому никаких дополнительных доказательств не будет. Будучи последним документом в расследовании, 2) он также является наиболее исчерпывающим документом, который служит источником доказательств. На этом фоне 3) SNA помогает сразу увидеть более широкую картину – показывая, кто важнее в сети – из длинных документов и 4) любое поведение и взаимодействие документируются в ордере на арест объективно и без каких-либо юридических ограничений. релевантность[464]. Эти преимущества обсуждаются ниже.

В Италии нет свидетельств использования этой СНС в расследованиях[465], но там, где использование инструментов анализа социальных сетей широко распространено в других полицейских силах, таких как Вирджиния (США), австралийская Виктория и Новый Южный Уэльс, эти преимущества четко видны, как уже упоминалось в литературе[466].

https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating.

Ордер на арест впервые раскрывает тот факт, что расследование продолжается. Юридическая природа документов уникальна[467]. Обычно ордер на арест является одним из самых первых документов, выдаваемых прокурором Италии в рамках любого уголовного процесса, и, как правило, последним документом каждого расследования вместе с уведомление о его окончании. В идеале каждое расследование приводит к выдаче ордера на арест, если имеется достаточно доказательств в поддержку обвинения. Постановление о заключении под стражу может быть издано прокурором при соблюдении ряда альтернативных условий: 1) имеются однозначные доказательства против подследственного; 2) существует риск того, что лицо может попытаться уйти от правосудия из-за наличия веских доказательств против него; 3) расследуемое преступление может быть наказано пожизненным тюремным заключением или тюремным заключением с минимум двумя годами тюремного заключения и

---

[464] Поскольку юридическая значимость действий и взаимодействий будет впоследствии оценена судьей.

[465] За исключением иерархического списка мафии / крупных преступных группировок (Falcone and Turone, 2015). Джованни Фальконе и Джулиано Туроне. «Tecniche di indagine in materia di mafia». Rivista di Studi e Ricerche sulla Criminalità organizationzata 1, no. 1 (2015): 116-153.

[466] Морган Бурчер и Чад Уилан. «Анализ социальных сетей как инструмент криминальной разведки: понимание его потенциала с точки зрения аналитиков разведки». Тенденции в организованной преступности 21, вып. 3 (2018): 278-294; Дженнифер Джонсон и др., «Анализ социальных сетей: систематический подход к исследованию». Бюллетень правоохранительных органов ФБР, (2013): 350.

[467] И часть литературы (Scaglione, 2011, Ficara et al., 2019, Musotto, 2016, Wall and Musotto, 2019) успешно использует ордера на арест в качестве отправной точки для анализа социальных сетей. Паоло Тонини, «Мануале пенальти» («Джуффре редактора», 2012 г.); Антонио Скальоне, мафиозный рети. Коза Ностра и Каморра: преступные организации противостоят (FrancoAngeli, 2011); Аннамария Фикара и др., «Анализ социальных сетей взаимосвязей сицилийской мафии». В Международной конференции по сложным сетям и их приложениям (Springer, Cham, 2019), 440-450; Роберто Мусотто, «Социальный и пространственный сетевой анализ организованной преступности». Докторская диссертация, Università degli Studi di Messina, (2016); Роберто Мусотто и Дэвид С. Уолл, «Являются ли Booter Services (Stressors) показателями новой формы организованной преступной группы в Интернете?» Журнал цифровой криминалистики 1, № 1 (2019): 41-50.

минимум шестью годами максимум, если оно касается терроризма или демократических подрывных действий (как это делают мафия или террористические преступления).

Однако наиболее важной особенностью ордера является то, что государственный прокурор по закону обязан представить все доказательства против и в пользу лица, в отношении которого в настоящее время проводится расследование. Это означает, что технически прокурор не имеет никаких реальных полномочий для отбора доказательств[468], потому что это будет сделано во время судебного разбирательства в состязательной манере, когда защита может представить другие доказательства для переосмысления или опровержения предполагаемого юридически значимого поведения. Все доказательства должны быть представлены судье, принимающим решение, прокурором, чтобы судья мог оценить положение подследственного[469] в свете имеющихся доказательств. На данном этапе прокурор может показать с помощью анализа социальных сетей: а) есть ли видимость структуры[470]; б) кто играет более важную роль в сети[471]; в) насколько связана группа.[472]

На предварительном слушании представляются все доказательства для анализа результатов расследования и для того, чтобы судья мог решить,

---

[468] Таким образом, единственными доказательствами, которые ему действительно разрешено отбросить, являются те, которые являются избыточными (например, двойные) или не имеют отношения (например, записи предполагаемого мафиози, не участвовавшего в преступных или подозрительных действиях) для расследования, как предписано законом № 332 от 1995 г. и Закон № 47 от 2015 г. Эту задачу по сбору всех доказательств, которые выступают в пользу и против исследуемого лица, чрезвычайно сложно выполнить во многих случаях, потому что, в конце концов, прокурор должен доказать основание предполагаемых обвинений . С точки зрения анализа социальных сетей это, тем не менее, может создать проблемы нечетких границ при определении преступной сети. Например, два человека сидят в машине, а один из них начинает говорить о компрометирующих фактах, таких как рэкет или встреча с другими подозреваемыми. Автомобиль прослушивается, и слушатель не известен как преступник. Следователи и прокурор, прослушивая этот разговор, должны сделать выбор: включать слушателя в преступную сеть или нет? Если да, они могут заподозрить, что он, вероятно, узнает больше или поделится дополнительной информацией в будущем. Это может привести к распространению преступной сети на людей, которые могут не быть ее частью, что приведет к необоснованному ущемлению их прав. В противном случае часть секретной сети может не быть раскрыта.

[469] Особенность этого источника заключается в том, что количество доступных данных для каждого узла (подключенного человека) и ссылки (взаимодействия) снижает риски потери данных внутри исследуемой сети при условии, что расследование было проведено тщательно. Даже если весь список ссылок внутри организации может быть не очевиден для следователей, вся наблюдаемая информация о каждой ссылке собирается вместе с помощью записей прослушивания телефонных разговоров, коллекций аудио и видео, генеалогических деревьев и документации. Таким образом, собранная информация должна быть как можно менее предвзятой. Впоследствии, в ходе судебного разбирательства, судья создаст меньшую сеть узлов и ссылок, которые подлежат уголовному наказанию. Тот факт, что ордер на арест является более полным, чем другие судебные акты на протяжении всего процесса и расследования, является причиной того, почему сетевой анализ будет полезен как для исследователей, так и для следователей.

[470] Это оценивается путем анализа типа связей каждого отдельного исследуемого человека.

[471] Это делается посредством анализа показателей центральности, поскольку они показывают, кто более важен в данной конкретной сети.

[472] 49 Это покажет наличие внутренних групп внутри группы, и это может быть сделано с помощью анализа клик или локального кластерного коэффициента. Первый изучает социальный круг и его связи по сравнению с остальной группой. Второй показывает, насколько вероятно, что некоторые люди (или объекты) связаны и могут стать кликой (в упрощенном примере, если A знает B, который знает C и D, вполне вероятно, что C и D знают друг друга или A).

достаточно ли доказательств для проведения судебного разбирательства против обвиняемого. Именно здесь можно использовать СНС, чтобы увидеть более широкую картину, но при этом она важна для отдельного обвиняемого. Судья должен убедиться, что собранные доказательства точно связаны с обвиняемым[473]. В таком контексте анализ динамического влияния узлов и связей[474], а также понимание центральности или гомофильных мер[475] были бы полезны, поскольку убедительный аргумент для оценки причастности отдельного лица к организации и ее значимости как преступного поведения, поскольку он позволил бы создать количественную меру против стандартного поведения, запрещенного законом.

Если судебное разбирательство продолжается, судья соберет доказательства у прокурора и защиты, и именно они решат, насколько веские доказательства против подсудимого, поскольку любые доказательства в пользу защиты могут действовать в противовес обвинениям. Судья – это орган, который делает выбор между доказательствами, позволяя рассматривать их как доказательство[476]. В этом ему помогает доведение доказательств до суда[477].

Суд завершается вынесением вердикта, который является результатом этой выборочной деятельности, что является еще одним моментом, в котором подходили бы методы анализа социальных сетей, потому что во всех этих преступлениях, в которых участвует организация[478] и группа, сеть должна быть «виртуально реконструирована»[479] судьей, и каждое доказательство оценивается с точки зрения его уголовной значимости. Результатом является не сама сеть, а сеть, имеющая отношение к уголовному законодательству. Таким образом, сеть, отображаемая судьей, сама по себе ограничена меньшей частью списка узлов и ссылок, который был впервые представлен судье[480]. В данном случае SNA сможет автоматизировать эту процедуру, как только порог будет установлен решающий судья.

Последняя сеть является результатом того, что имеет криминальное значение, т.е. того, что заслуживает наказания в соответствии с уголовным

---

[473] Например, судья на предварительном слушании может рассмотреть меры центральности СНС и установить числовой порог, чтобы решить, кого возбуждать или нет, а также иметь возможность требовать дальнейшего расследования или прекращения дела для тех лиц, которые не соответствуют таким требованиям.

[474] Стивен П. Боргатти и др., «Сетевой анализ в социальных науках». Наука 323, вып. 5916 (2009): 892-895.

[475] Мартин Нёклеберг, «Изучение принципов множественной полицейской деятельности: переход от нормативных дебатов к эмпирическим исследованиям». Британский журнал криминологии, (2020). DOI: https://doi.org/10.1093/bjc/azz080

[476] Или присяжных по конкретным преступлениям и судебным процессам (например, преступлениям против человечности).

[477] Которые перечислены в статьях 194–243 Уголовно-процессуального кодекса Италии.

[478] Даже минимальный.

[479] Судья воссоздает структуру сети на основании имеющихся перед ним доказательств.

[480] Джулия Берлускони и др., «Предсказание связей в криминальных сетях: инструмент для анализа криминальной разведки». PloS one 11, no. 4 (2016). doi: https://doi.org/10.1371/journal.pone.0154244.

законодательством[481]. На самом деле, для судебного органа важно то, что все доступные доказательства об организации преступления и преступнике организация настроена на суждение.

После того, как судья кристаллизует сеть и вынесет вердикт, процесс повторного выбора узлов и ссылок может быть повторен в двух следующих апелляциях. Основное отличие от первого испытания с точки зрения сетевого анализа состоит в том, что невозможно представить новые доказательства в суд и, следовательно, создать новое доказательство.[482] В апелляции есть два возможных сетевых результата: размер и связи подтверждены или некоторые обвиняемых могут быть оправданы судом с сокращением сети до меньшей доли. На заключительном этапе, когда все средства обжалования исчерпаны или истекли, приговоры должны быть приведены в исполнение с целью перевоспитания правонарушителя в свете его социальной реабилитации[483].

Вывод

Целью данной статьи было выяснить, подходит ли, где и как анализ социальных сетей в судебной системе. Используя нынешнюю организацию итальянских уголовных судов, он позволяет определить несколько областей, на которых следует сосредоточить будущую практику и исследования: 1) в качестве инструмента убеждения в конце расследования; 2) как средство превращения доказательств в доказательства в ходе судебного разбирательства и 3) как инструмент для судей при выборе криминальной сети.

---

[481] По мнению исследователей, именно поэтому приговор менее склонен к анализу или реконструкции сети, чем ордер на арест. В этом последнем документе доказательства отображаются в необработанном формате и еще не были отфильтрованы с помощью процедуры шлифования судебного решения, которая является условным процессом. Следовательно, ордер на арест имеет интересные особенности для сбора качественных данных о преступных сетях для сетевого анализа. Это так, потому что, несмотря на то, что это вторичный источник, который может иметь неправильную атрибуцию в том, как формируются и создаются узлы и связи (Campana, 2016), способ написания ордера может уменьшить проблемы с недостающими данными. Паоло Кампана, «Объяснение преступных сетей: стратегии и потенциальные ловушки». Методологические инновации 9, (2016).

[482] Если они не были обнаружены после окончания первого судебного разбирательства, предусмотренного статьей 603 Уголовно-процессуального кодекса.

[483] Это еще одна область, в которой СНС может помочь. Заключенные продолжают общаться во время пребывания в тюрьме, и их влияние в сети может иметь положительные или отрицательные последствия для рецидивизма (Berg and Huebner, 2011; Duwe and Clark, 2013). Марк Т. Берг и Бет М. Хюбнер. «Возвращение и узы, которые связывают: изучение социальных связей, занятости и рецидивизма». Правосудие ежеквартально 28, вып. 2 (2011): 382-410; Грант Дьюв и Валери Кларк. «Благословенны социальные связи, связывающие: влияние посещения тюрьмы на рецидив преступников». Обзор политики в области уголовного правосудия 24, no. 3 (2013): 271-296. и расширение преступной сети (Tremblay, 2017). Пьер Трембле, «В поисках подходящих соучастников». В рутинной деятельности и рациональном выборе под ред. (Р.В.Г. Кларк и Маркус Фелсон, Routledge, 2017 г.), 17–36. Таким образом, СНС можно использовать для прогнозирования (Gravel and Tita, 2015), кто может подвергаться более высокому риску, глядя на связи и взаимодействия. Джейсон Гравел и Джордж Э. Тита. «Хорошие методы влекут за собой большие обязанности: анализ социальных сетей при реализации и оценке программ банд». Криминология и паб. Политика 14, номер 3 (2015): 559-527.

Анализ социальных сетей в суде служит двум целям: 1) систематизировать и систематизировать объем разведданных, собранных в ходе расследования над группой лиц[484], и в то же время 2) упростить и автоматизировать деятельность прокуроров и судей в создании доказательств во время судебного разбирательства, учитывая жесткие процедурные временные рамки[485] и заведомо чрезмерная продолжительность судебных разбирательств[486]. Преимущество использования СНС в судах заключается в том, что она экономит время и, следовательно, снижает затраты на управление судебным процессом. Это также проясняет более широкую картину расследования, в то же время имея возможность измерить участие человека в поддающемся количественной оценке вопросе.

Недостатки состоят в том, что анализ может быть необъективным, так как полная информация недоступна; есть вопрос о границах (кого включать в сеть); и можно предвидеть отсутствие желания воспользоваться преимуществами СНС из-за нехватки цифровых навыков в этом секторе. Все эти предубеждения необходимо дополнительно изучить с помощью практических и качественных исследований до их внедрения. Чтобы облегчить использование методов СНС, обучение экспертов в области права имеет решающее значение для ее успешного применения в методах и практике расследования, как это уже происходит в некоторых юридических контекстах по всей Европе[487].

[484] Автор, интервью с офицером полиции Валенсии, февраль 2018 г.
[485] Автор, интервью с прокурором Нидерландов, сентябрь 2018 г.
[486] Это верно для большинства европейских стран. Чрезмерная продолжительность судебного разбирательства является основной причиной подачи жалоб в Европейский суд по правам человека о нарушении статьи 6 его договора (CEPEJ, 2016). Совет Европы, Европейская комиссия по эффективности правосудия (CEPEJ). «Отчет о европейских судебных системах, эффективности и качестве правосудия». CEPEJ Исследования нет. 23 (2016).
[487] Прокуратуры и судьи в Нидерландах и Испании только начали проходить обучение анализу социальных сетей после получения квалификации.

Ссылки

Болл, Лесли. «Автоматизация анализа социальных сетей: мощный инструмент борьбы с терроризмом». Журнал безопасности 29, вып. 2 (2016): 147-168.

Берг, Марк Т. и Бет М. Хюбнер. «Возвращение и связывающие узы: исследование социальных связей, занятости и рецидивизма». Правосудие ежеквартально 28, вып. 2 (2011): 382-410.

Берлускони, Джулия. «Все ли части имеют значение? Оценка надежности источников данных правоохранительных органов для сетевого анализа прослушиваний ». Глобальная преступность 14, № 1 (2013): 61-81.

Берлускони, Джулия, Франческо Кальдерони, Никола Паролини, Марко Верани и Карло Пиккарди. «Предсказание ссылок в криминальных сетях: инструмент для анализа криминальной разведки». PloS one 11, no. 4 (2016). doi: https: //doi.org/10.1371/journal.pone.0154244.

Бесоу, Лоуренс М., Джефф К. Ву, Чо Й. Чанг, Даррен Д. Смит и Марк Дж. Кин. «Графическое отображение топологии сети». Патент США 5,276,789, поданный 14 мая 1990 г. и выданный 4 января 1994 г.

Боргатти, Стивен П., Аджай Мера, Даниэль Дж. Брасс и Джузеппе Лабьянка. «Сетевой анализ в социальных науках». Наука 323, вып. 5916 (2009): 892-895.

Брайт, Дэвид А., Кейтлин Э. Хьюз и Дженни Чалмерс. «Освещение темных сетей: анализ социальных сетей австралийского синдиката незаконного оборота наркотиков». Преступность, закон и социальные изменения 57, вып. 2 (2012): 151-176.

Бурчер, Морган и Чад Уилан. «Анализ социальных сетей как инструмент криминальной разведки: понимание его потенциала с точки зрения аналитиков». Тенденции в организованной преступности 21, вып. 3 (2018): 278-294.

Кальдерони, Франческо. «Структура мафии наркобизнеса:« Ндрангета и кокаин». Преступность, закон и социальные изменения 58, вып. 3 (2012): 321-349.

Кампана, Паоло. «Объяснение преступных сетей: стратегии и потенциальные ловушки». Методологические инновации 9, (2016).

Кампана, Паоло и Федерико Варезе. «Прослушивание проводов: критерии и методы количественного анализа перехвата телефонных

разговоров». Тенденции в организованной преступности 15, вып. 1 (2012): 13-30.

Кэррингтон, Питер Дж. (2011) «Анализ преступности и социальных сетей». Справочник SAGE по анализу социальных сетей: 236-255.

Чапхалкар Н.Б. и Саяли С. Сандбхор. «Применение нейронных сетей в разрешении споров по вопросу об эскалации с использованием нейро-решений». KSCE Журнал гражданского строительства 19, вып. 1 (2015): 10-16.

Колладон, Андреа Фронцетти и Элиза Ремонди. «Использование анализа социальных сетей для предотвращения отмывания денег». Экспертные системы с приложениями 67 (2017): 49-58.

Совет Европы, Европейская комиссия по эффективности правосудия (CEPEJ). «Отчет о европейских судебных системах, эффективности и качестве правосудия». CEPEJ Исследования нет. 23, (2016).

Дэвис, Роджер Х. «Анализ социальных сетей: помощь в расследовании заговоров». ФБР L. Enforcement Bull 50, (1981): 11.

Duijn, Paul AC и Peter PHM Klerks. «Анализ социальных сетей применительно к криминальным сетям: последние события в правоохранительной сфере Нидерландов». В Сети и сетевой анализ для защиты и безопасности, стр. 121-159. Спрингер, Чам, 2014.

Дуве, Грант и Валери Кларк. «Благословенны социальные связи, связывающие: влияние посещения тюрьмы на рецидив преступников». Обзор политики в области уголовного правосудия 24, no. 3 (2013): 271-296.

Фабиан, Седа. «Искусственный интеллект и закон: будут ли судьи работать на перфокартах». Общий L. Rev.16 (2020): 4.

Фальконе, Джованни и Джулиано Туроне. «Tecniche di indagine in materia di mafia». Rivista di Studi e Ricerche sulla Criminalità organizationzata 1, no. 1 (2015): 116-153.

Фикара, Аннамария, Люсия Кавалларо, Паскуале де Мео, Джакомо Фьюмара, Сальваторе Катанезе, Овидиу Багдасар и Антонио Лиотта. «Анализ социальных сетей взаимосвязей сицилийской мафии». В Международной конференции по сложным сетям и их приложениям. Спрингер, Чам, 2019, 440-450.

Гарофоли, Винченцо. Diritto processuale penale. Джуффре Эдиторе, (2008).

Гравий, Джейсон и Джордж Э. Тита. «Хорошие методы влекут за собой большие обязанности: анализ социальных сетей при реализации и оценке программ банд». Криминология и паб. Политика 14, вып. 3 (2015): 559-527.

Ху, Пол Джен-Хва, Синьчунь Чен, Хан-фен Ху, Кэти Ларсон и Синтия Бутирес. «Принятие сотрудниками правоохранительных органов передовых технологий электронного правительства: исследование COPLINK Mobile». Исследования и приложения электронной торговли 10, вып. 1 (2011): 6-16.

Джонсон, Дженнифер, Джон Дэвид Рейцель, Б. Норвуд, Д. Маккой, Б. Камминг и Р. Тейт. «Анализ социальных сетей: систематический подход к расследованию». Бюллетень правоохранительных органов ФБР, (2013): 350.

https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating.

Кельзен, Ганс. Чистая теория права. Беркли: Калифорнийский университет Press, 1967.

Климанс, Эдвард Р. и Кристиан Дж. Де Пут. «Криминальная карьера в организованной преступности и структура социальных возможностей». Европейский журнал криминологии 5, вып. 1 (2008): 69-98.

Косинец, Георги. «Последствия отсутствия данных в социальных сетях». Социальные сети 28, №1. 3 (2006): 247-268.

Косинец, Георги и Дункан Дж. Уоттс. (2006). «Эмпирический анализ развивающейся социальной сети». Наука 311, вып. 5757, 88-90.

Кребс, Валдис Э. «Картографирование сетей террористических ячеек. «Связи 24, нет. 3 (2002): 43-52.

Лу, Юн, Синь Ло, Майкл Полгар и Юаньюань Цао. «Анализ социальных сетей криминального хакерского сообщества. «Журнал компьютерных информационных систем 51, вып. 2 (2010): 31-41.

Морено, Джейкоб Леви. Первая книга по групповой психотерапии. Монографии по психодраме и групповой психотерапии 1, Beacon House, 1957.

Морено, Джейкоб Леви. Применение группового метода к классификации. Нью-Йорк: Национальный комитет по тюрьмам и тюремному труду, 1932.

Морселли, Карло. 2009. Внутри криминальных сетей (Том 8). Нью-Йорк: Спрингер.

Мусотто, Роберто. «Социальный и пространственный сетевой анализ организованной преступности». Кандидатская диссертация, Università degli Studi di Messina, 2016.

Мусотто, Роберто и Дэвид С. Уолл. «Указывают ли Booter Services (Stressors) на новую форму организованной преступной группы в Интернете?» Журнал цифровой криминалистики 1, № 1 (2019): 41-50.

Натараджан, Мангай. «Понимание структуры крупной сети распространения героина: количественный анализ качественных данных». Журнал количественной криминологии 22, вып. 2 (2006): 171-192.

Нёклеберг, Мартин. «Изучение того, как действует множественное число полицейских: переход от нормативных дебатов к эмпирическим исследованиям». Британский журнал криминологии, (2020). doi: https://doi.org/10.1093/bjc/azz080

Петерсен, Расмус Розенквист, Кристофер Дж. Родс и Уффе Кок Виль. «Удаление узлов в криминальных сетях». В 2011 г. Европейская конференция по разведке и информатике безопасности, изд. Персонал IEEE, 360-365. IEEE, (2011).

Пикеро, Алекс. Р. изд. Справочник криминологической теории. Джон Вили и сыновья, 2015.

Очки, Лори и Поттон, Под ред. «Искусственный интеллект и автоматизация в Великобритании». Информационный документ: 8152 (2017).

Руткин, Авива. «Судья - робот». New Scientist 222: 2973, нет. 24 (2014).

47

Скальоне, Антонио. Reti mafiose. Cosa Nostra e Camorra: преступные организации противостоят. Франко Анджели, 2011.

Шредер, Дженнифер (2001). Департамент полиции Тусона и Соединенных Штатов Америки. «COPLINK: интеграция базы данных и доступ к интранету правоохранительных органов, окончательный отчет». Вашингтон, округ Колумбия: Министерство юстиции США

Зиммель, Георг. «Проблема социологии». Американский журнал социологии 15 номер 3 (1909): 289-320.

Сурдин, Таня. (2018). «Судья против робота: искусственный интеллект и принятие судебных решений». UNSWLJ 41, нет. 4 (2018): 1114.

Воробей, Малькольм. К. «Применение сетевого анализа к криминальной разведке: оценка перспектив». Соцсети 13 нет. 3 (1991): 251-274.

Сазерленд, Эдвин Х., Дональд Р. Кресси и Дэвид Ф. Лакенбилл. Принципы криминологии. Лэнхэм: AltaMira Press, 1992.

Тонини, Паоло. Manuale di scheme penale. Giuffrè editore, 2012.

Трембле, Пьер. «Поиск подходящих соучастников». В рутинной деятельности и рациональном выборе под ред. Р.В.Г. Кларк и Маркус Фелсон, Routledge, 2017. 17–36.

Ван дер Халст, Рене К. «Введение в анализ социальных сетей (SNA) как инструмент расследования». Тенденции организованной преступности 12, вып. 2 (2009): 101-121.

Ёнтэ Пак и Юн, Бёнгун. «Патентная сеть на основе интеллектуального анализа текста: аналитический инструмент для выявления тенденций в области высоких технологий». Журнал исследований в области управления высокими технологиями15, вып. 1 (2004): 37-50.

Искусственный интеллект в здравоохранении: оценка рисков и уголовное право

Федерико Кармело Ла Ваттиата

Достижения в области искусственного интеллекта (ИИ) меняют характер медицинской помощи. Они охватывают как диагностику, так и терапию. В медицинской литературе широко анализируются преимущества и риски ИИ. Исследователи обнаружили, что ранняя диагностика необходима для предотвращения ухудшения состояния здоровья пациентов. Это может быть достигнуто за счет улучшения процедур анализа медицинских данных с помощью методов искусственного интеллекта. Однако, чтобы гарантировать безопасность медицинских устройств с искусственным интеллектом, их клиническая оценка имеет решающее значение.

Данная статья направлена на концептуализацию и решение вопросов, связанных с применением искусственного интеллекта в здравоохранении с точки зрения уголовного права. Будут исследованы традиционные категории уголовного права, чтобы понять, можно ли рассматривать смерть и травмы, происшедшие в контексте оказания медицинской помощи, как уголовные преступления, которые необходимо предотвращать и преследовать в судебном порядке при использовании методов искусственного интеллекта. Исследование будет проводиться в сравнительной перспективе. В заключение, это позволит предложить новую парадигму оценки рисков ИИ, основанную на интеграции мер уголовного, гражданского и административного права, чтобы гарантировать равновесие между основными правами обвиняемого (справедливое судебное разбирательство) и потерпевших (компенсация за понесенный ущерб).

Ключевые слова: ИИ, здравоохранение, риск, уголовное право.

Вступление

Достижения в области искусственного интеллекта меняют характер медицинской помощи. Под ИИ понимаются «системы, которые демонстрируют разумное поведение, анализируя окружающую среду и предпринимая действия – с некоторой степенью автономии – для достижения определенных целей. Системы на основе ИИ могут быть чисто программными, действующими в виртуальном мире или ИИ может быть встроен в аппаратные устройства»[488]. Другими словами, интеллектуальная система состоит из набора алгоритмов, которые могут использовать данные для решения (более или менее сложные) проблемы в разных контекстах.

Следует уточнить фундаментальную технику в области ИИ, то есть машинное обучение (ML). Последний основан на сложных математических методах, поскольку связанные представления знаний включают теорию вероятностей и статистику. Искусственные нейронные сети (ИНС) являются ключевыми элементами. Это нейронные вычислительные системы, вдохновленные функционированием человеческого мозга, то есть биологические нейронные сети (BNN). В частности, между ними есть два сходства. Во-первых, строительные блоки обеих сетей представляют собой сильно взаимосвязанные вычислительные «инструменты». Во-вторых, ИНС состоят из вычислительных сетей, которые распределены параллельно и функционируют как различные синаптические силы биологических нейронов:

Комиссия ЕС. Искусственный интеллект для Европы, Сообщение Комиссии Европейскому парламенту, Европейскому совету, Европейскому экономическому и социальному комитету и Комитету регионов[489], (25 апреля 2018 г.).

Много входных сигналов к нейронам, и влияние каждого входа зависит от присвоенного ему веса, а именно адаптивного коэффициента в сети, который определяет интенсивность входного сигнала. В заключение, «выходной сигнал нейрона создается блоком суммирования, примерно соответствующим телу биологической клетки, который алгебраически складывает все взвешенные входные данные».

---

[488] Федерико Кармело Ла Ваттиата - аспирант в области сравнительных и европейских исследований (уголовное право) Университета Тренто, Италия.

[489] 2 Парк Янг-Сеук и Сован Лек, «Искусственные нейронные сети: многослойный персептрон для экологического моделирования», Developments in Environmental Modeling, 28 (2016): 124, https://doi.org/10.1016/B978-0-444-63623 -2.00007-4.

Есть три вида машинного обучения:

1. Контролируемое обучение, при котором программист обучает систему, определяя набор ожидаемых результатов по отношению к определенному диапазону входных данных и постоянно оценивая достижения целей. Затем система формулирует гипотезу. Каждый раз, когда он делает ошибку, гипотеза пересматривается;

2. Обучение без учителя, при котором пользователь не предоставляет ни ожидаемых результатов, ни отчетов об ошибках;

3. Обучение с подкреплением, при котором система управляется своего рода механизмом вознаграждения-наказания, то есть сообщениями обратной связи о том, что было сделано хорошо или плохо. В сложных ситуациях об успехе или неудаче системы сообщается после множества решений, и своего рода процедура присвоения кредитов определяет решения, которые, вероятно, приведут к успеху.

Другой важный метод – это так называемое глубокое обучение (DL), подмножество ML: это метод, который позволяет машинам лучше определять закономерности за счет более сложного использования нейронных сетей. Благодаря этой характеристике можно распознавать шаблоны данных на различных иерархических уровнях. Другими словами, DL может идентифицировать многоуровневое представление знаний.

Короче говоря, алгоритмы машинного обучения используют статистику и математику для поиска закономерностей и корреляций в больших данных[490]. Чем больше система обрабатывает данные, тем больше она улучшается. Следовательно, важно задержание больших данных. Очень немногие физические и юридические лица владеют этим новым видом богатства. Это связано с появлением новой власти, которую особенно трудно контролировать и ограничивать с помощью традиционных средств. По этой причине необходимы новые системы сдержек и противовесов, чтобы сбалансировать два интереса: а) продвигать выгодные разработки ИИ; и б) для предотвращения злоупотреблений, которые могут создать угрозу правам личности[491].

В целом существует четыре критерия классификации рисков и возможностей, связанных с использованием ИИ. Когда ИИ используется правильно, он позволяет человеку саморегулироваться и действовать, а также

---

[490] Определение «больших данных» таково: очень большие наборы данных, которые создаются людьми, использующими Интернет, и которые могут быть сохранены, поняты и использованы только с помощью специальных инструментов и методов.
См. Https://dictionary.cambridge.org/it/dizionario/inglese/big-data.

[491] Карло Касонато, «Potenzialità e sfide dell'intelligenza artificiale», BioLaw Journal, 1 (2019): 178.

улучшать общественный потенциал и сплоченность. Вместо этого, когда ИИ используют не по назначению или злоупотребляют, он снижает компетенцию людей, снимает с них ответственность и недооценивает их навыки самоконтроля и самоопределения[492].

Принципы этики надежного искусственного интеллекта

В 2018 году Европейская комиссия создала независимую группу экспертов высокого уровня по искусственному интеллекту (AI HLEG), которая опубликовала документ под названием «Этические рекомендации для надежного искусственного интеллекта» с целью продвижения надежного ИИ.

Согласно документу, «надежность является необходимым условием для людей и общества при разработке, развертывании и использовании систем ИИ»[493]. Надежный ИИ должен быть: a) законным; б) этический; и c) надежный.

Документ обеспечивает основу для создания заслуживающего доверия ИИ, основанного на фундаментальных правах, закрепленных в Хартии основных прав Европейского Союза, и соответствующих международных гуманитарных прав, прав человека, такого как Европейская конвенция о правах человека. Кроме того, в документе изложены три серии ключевых указаний. Во-первых, он «определяет этические принципы и соответствующие им ценности, которые должны соблюдаться при разработке, развертывании и использовании систем ИИ»: a) уважение к автономии человека, предотвращение вреда, справедливость и объяснимость; б) необходимость уделять внимание ситуациям с участием более уязвимых групп, а также ситуациям, которые характеризуются асимметрией власти или информации; и c) признание рисков, связанных с искусственным интеллектом (включая воздействия, которые может быть трудно предвидеть, идентифицировать или измерить), и принятие адекватных мер по их снижению. Во-вторых, дается руководство о том, как можно реализовать заслуживающий доверия ИИ, и для этой цели перечисляются семь ключевых требований, которым должны соответствовать системы ИИ: i) участие и контроль со стороны человека; ii) техническая надежность и безопасность; iii) конфиденциальность и управление данными; iv) прозрачность; v) разнообразие недискриминация и справедливость; vi) экологическое и социальное благополучие; и vii)

---

[492] Лучано Флориди, Джош Коулс, Моника Бельтраметти, Раджа Шатила, Патрис Чазеран, Вирджиния Дигнум, Кристоф Лютге, Роберт Мадлен, Уго Пагалло, Франческа Росси, Буркхард Шафер, Пегги Валке и Эффи Вайена, «AI4People - хороший этический фреймворк Общество: возможности, риски, принципы и рекомендации », Умы и машины 28, 4 (2018): 689-707,

[493] Группа экспертов ЕС высокого уровня по ИИ, Этические рекомендации для надежного ИИ, 4 (8 апреля 2019 г.),

подотчетность. Наконец, в документе представлен список оценок, который необходимо будет адаптировать к конкретному варианту использования системы ИИ.

Как мы увидим в следующем абзаце, ИИ может широко применяться в медицине, и его потенциальный вклад в эту область кажется безграничным. Однако могут возникнуть этические проблемы, учитывая, что интеллектуальные системы обладают огромной способностью угрожать предпочтениям, безопасности и конфиденциальности пациентов. Преимущества и риски, связанные с применением ИИ в здравоохранении, должны быть тщательно сбалансированы[494]. Кроме того, могут возникнуть вопросы уголовного права в отношении области врачебной халатности, такие как проблемы с черным ящиком, касающиеся этиологической связи между использованием ИИ и повреждениями, а также трудности с определением правил предосторожности, виновное нарушение которых оправдывает осуждение за грубую халатность или безрассудство.

ИИ в здравоохранении

В 1959 году эксперты начали дискутировать на тему трудных решений в сложных клинических ситуациях с помощью компьютеров.

ИИ в здравоохранении включает в себя как диагностику, так и терапию[495]. Приложения разнообразны: от мобильных приложений для постановки диагноза до хирургических роботов[496]. Рекламная гипербола медицинских устройств с ИИ «привела к скептицизму и непониманию того, что такое и невозможно» с ML[497]. Следует исследовать причины сомнений в достоверности, которые влияют на принятие систем поддержки клинических решений (CDSS). Есть сложности, которые ограничивают возможность быстрого продвижения вперед. Они отражают клиническую практику: а) черные ящики недопустимы, поскольку CDSS требует прозрачности; б) время – дефицитный ресурс, учитывая, что CDSS должен быть «эффективным с точки зрения требований ко времени и должен вписываться в рабочий процесс

---

[494] Майкл Дж. Ригби, «Этические аспекты использования искусственного интеллекта в здравоохранении», AMA J Ethics 21, 2 (2019): 121-124, https://journalofethics.ama-assn.org/article/ethical-dimensions- с использованием искусственного интеллекта-здравоохранения / 2019-02.

[495] Внутри рода «терапевтические средства» можно выделить три вида: а) лечебная терапия; б) хирургическая терапия; в) смешанная терапия (например, некоторые новообразования необходимо лечить с помощью: во-первых, онкологического вмешательства, чтобы уменьшить критическую массу; во-вторых, хирургического вмешательства для ее удаления; и, наконец, другого онкологического вмешательства для предотвращения риск метастазирования).

[496] Однако недавние исследования сравнивали уровень диагностической.

[497] Сучи Сария, Атул Бьютт и Азиз Шейх, «Лучшая медицина через машинное обучение: что реально, а что искусственно?», PloS Med. 15, 12 (2018): 1, https://doi.org/10.1371/journal.pmed .1002721.

загруженной клинической среды»; c) «сложность и отсутствие удобства использования препятствуют использованию», поскольку CDSS «должен быть интуитивно понятным и простым для изучения и использования»; г) «актуальность и понимание важны», фактически «CDSS должен отражать понимание соответствующей области и видов вопросов, с которыми клиницисты могут нуждаться в помощи»; e) предоставление знаний и информации должно быть уважительным, и CDSS «должен предлагать совет таким образом, чтобы признавать опыт пользователя, давая понять, что он предназначен для информирования и помощи, но не для замены клинициста»; и, наконец, f) научная база должна быть прочной, поскольку CDSS «должен иметь строгие, прошедшие экспертную оценку научные данные, подтверждающие его безопасность, валидность, воспроизводимость, удобство использования и надежность» эффективности людей и систем искусственного интеллекта. Результатом стала победа людей. Разброс между выборками прямо пропорционален редкости болезней: чем более нетипичное заболевание, тем больше люди используют свои личные навыки, поскольку клинический вопрос не может быть решен просто с помощью статистики. Вместо этого, когда болезнь является обычным явлением, системы ИИ могут использовать свои (потенциально безграничные) навыки в обработке данных[498].

Хотя человеческие врачи не могут быть заменены системами ИИ в обозримом будущем, ИИ может сыграть ключевую роль в оказании помощи врачам в принятии более эффективных клинических решений. В некоторых случаях интеллектуальные системы могут даже заменить человеческое суждение в определенных областях здравоохранения.

Фактически, большой объем медицинских данных может быть эффективно вычислен с помощью алгоритмов искусственного интеллекта, чтобы помочь клинической практике. Интеллектуальные системы могут быть оснащены обучающими и самокорректирующимися навыками для повышения их точности и поддержки врачей в сокращении диагностических и терапевтических ошибок. Более того, системы искусственного интеллекта могут использоваться для извлечения информации из большого числа пациентов и оказания помощи в создании выводов в реальном времени для предупреждения о риске для здоровья и прогнозирования результатов[499].

Медицинские устройства с искусственным интеллектом можно разделить на две категории: a) методы машинного обучения, которые анализируют

---

[498] См. Hannah L. Semigran, David M. Levine, Shantanu Nundy и Ateev Mehrotra, «Сравнение терапевтической и компьютерной точности диагностики», JAMA Internal Medicine 176, 12 (2016): 1860-1861, https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2565684.

[499] Фей Цзян, Юн Цзян, Хуэй Чжи, И Донг, Хао Ли, Суфенг Ма, Илун Ван, Цян Донг, Хайпенг Шен и Юнцзюнь Ван, «Искусственный интеллект в здравоохранении: прошлое, настоящее и будущее», Инсульт и сосудистая неврология 2, 4 (2017): 230, http://dx.doi.org/10.1136/svn-2017-000101.

медицинские данные (например, изображения, генетические данные и данные ЕР) с целью группирования характеристик пациентов или определения вероятности исхода определенных заболеваний; б) методы обработки естественного языка (НЛП), которые обрабатывают неструктурированные данные (например, клинические заметки и медицинские журналы) с целью разработки структурированных медицинских данных. В частности, DL очень эффективен при интерпретации данных в виде изображений в силу сложности факторов, которые он может учитывать.

В медицинской литературе широко обсуждаются преимущества искусственного интеллекта, в основном в отношении трех типов заболеваний: сердечно-сосудистых заболеваний, рака и болезней нервной системы. Это основные причины смерти. Таким образом, ранняя диагностика важна для предотвращения ухудшения состояния здоровья пациентов. Это может быть достигнуто за счет улучшения процедур анализа медицинских данных с помощью методов искусственного интеллекта.

При этом все еще предстоит решить несколько проблем. Во-первых, в действующих правилах отсутствуют стандарты для оценки безопасности и эффективности систем ИИ. Кроме того, ученые занимаются проблемами обмена данными. С этой точки зрения следует учитывать, что интеллектуальные системы необходимо постоянно обучать с помощью клинических данных: первое обучение может быть основано на исторических наборах данных; однако следующие шаги требуют продолжения информации. Это важный вопрос для развития и улучшения системы[500].

Вопросы уголовного права, возникающие в связи с использованием ИИ в здравоохранении

Многие вопросы в области уголовного права возникают в связи с разработкой программного обеспечения как медицинского устройства (SaMD). Вкратце нам необходимо уточнить:

1. Должны ли системы ИИ рассматриваться как агенты, поскольку они могут быть юридическими лицами, или просто инструменты, с помощью которых люди могут совершать преступления;

2. Как преступления с использованием искусственного интеллекта (AIC)– т.е. преступления с использованием системы искусственного интеллекта – могут осуществляться в области медицинских устройств, а именно являются ли они преступлениями, обычно основанными на конкретном поведении или требующими наступления определенного события[501]; также в последнем случае

---

[500] Фэй Цзян и др., Иви, 241.

[501] Томас К. Кинг, Никита Аггарвал, Мариаросария Таддео и Лучано Флориди, «Преступление с применением

как мы можем решить вопросы, касающиеся этиологической связи между поведением агента и событием, а также разновидностей вины;

3. Наконец, можно ли теоретизировать новую более справедливую модель.

Объекты AI как юридические лица

Габриэль Халлеви теоретизировал возможные формы уголовной ответственности систем искусственного интеллекта, основанные на присвоении им правосубъектности. Он постулировал три модели:

1. Модель «преступление через другую», где система ИИ рассматривается как невиновный агент, простой инструмент, используемый фактическим преступником (принципалом), то есть программистом или пользователем;

2. Модель «естественные – вероятные последствия», в которой программисты или пользователи могут быть привлечены к уголовной ответственности за преступление, совершенное с помощью ИИ и являющееся естественным и вероятным следствием их преднамеренного или небрежного поведения;

3. Модель прямой ответственности, в которой предполагается, что ИИ наделен mens rea и, следовательно, совместим с бременем ответственности за поведение, которое в материальном плане осуществляется им самим.

В последней модели Халлеви выдвигает гипотезу о возможном применении наказания, построенном в соответствии с принципом эквивалентности между машиной и человеком. Речь идет об удалении программного обеспечения с намерением нейтрализовать систему или отключении ее на заранее установленный период времени, чтобы способствовать ее перевоспитанию. Тем не менее, третья модель Халлеви неприемлема. Он основан на ошибочных аргументах.

Во-первых, системы ИИ на самом деле неразумны. По закону домыслы без научных доказательств не могут служить действительной ссылкой. Как утверждает Лучано Флориди, профессор Оксфордского института Интернета, лучшим определением ИИ по-прежнему остается то, что дал Джон Маккарти в 1955 году: проблема ИИ «рассматривается как проблема заставить машину вести себя так, как это можно было бы назвать разумным, если бы человек вел

искусственного интеллекта: междисциплинарный анализ прогнозируемых угроз и решений», Sci. Англ. Этика 26, (2020): 90-91, https://doi.org/10.1007/s11948-018-00081-0.

себя так»[502]. Таким образом, мы можем назвать такое поведение разумным, поскольку человек ведет себя таким образом, но это не означает, что машина разумна[503].

Халлеви утверждает, что возражения против уголовной ответственности субъектов AI (прежде всего в отношении требования mens rea) основаны на аргументах, аналогичных тем, которые касаются ответственности корпораций. Тогда не было бы «существенной юридической разницы между идеей уголовной ответственности, налагаемой на корпорации и объекты ИИ». Тем не менее, есть существенная разница: «согласно правилу «вышестоящего агента», корпоративная уголовная ответственность ограничивается ситуациями, в которых поведение осуществляется или в которых участвует совет директоров или высокопоставленный управленческий агент[504]. Напротив, третья модель Халлеви «не предполагает никакой зависимости сущности Al от конкретного программиста или пользователя»[505].

Наконец, уголовная ответственность основана на двух ключевых концепциях правонарушения и атрибуции[506], которые предполагают два необходимых условия:

1.Человеческое (и добровольно совершенное) действие или бездействие[507] (также известное как actus reus)[508];

2.mens rea (разновидности вины), т. е. действие / бездействие должно быть покрыто чувством вины.

---

[502] Джон Маккарти, Марвин Л. Мински, Натаниэль Рочестер и Клод Э. Шеннон, «Предложение для Дартмутского летнего исследовательского проекта по искусственному интеллекту; 31 августа 1955 г. »AI Magazine 27, 4 (2006): 12, https://doi.org/10.1609/aimag.v27i4.1904.

[503] Лучано Флориди, «Раскалывающая сила цифровых технологий и ее последствия», Philos. Technol. 30, (2017): 123-129,
https://doi.org/10.1007/s13347-017-0259-1.
Автор утверждает, что если бы кто-то утверждал, что машина разумна, это было бы «заблуждением, имеющим привкус суеверия (сравните: река достигает озера, следуя наилучшим возможным путем, устраняя препятствия на своем пути; если бы это было сделано путем кого-то, мы сочли бы такое поведение разумным; значит, поведение реки разумное) ».

[504] Уэйн Р. Лафэйв и Остин В. Скотт-младший, Материальное уголовное право, Том 1 (Сент-Пол - Миннесота: West Publishing Co., 1986), 360.

[505] Габриэль Халлеви, «Уголовная ответственность субъектов искусственного интеллекта - от научной фантастики до правового социального контроля», Akron Intellectual Property Journal 4, 2, статья 1 (2010): 186, http://ideaexchange.uakron.edu/akronintellectualproperty/ vol4 / iss2 / 1.

[506] Действие считается противоправным, если оно удовлетворяет определению преступления и является необоснованным. Определение преступления состоит из набора (объективных и субъективных) элементов, которые составляют так называемое инкриминирующее дело обвиняемого. Это предусмотрено базовой нормой, то есть нормой, адресованной гражданам, которая запрещает определенные действия или требует выполнения определенных действий. Таким образом, они возлагают на физических лиц обязанности соблюдения. Следовательно, понятие противоправного поведения является формальным, поскольку определяется несовместимостью деяния с нормами правовой системы. Напротив, концепция правонарушения является существенной: сказать, что правонарушитель является правонарушителем (или что он / она участвовал в правонарушении), означает вынести суждение о внутреннем качестве его / ее деяний. К концепции атрибуции можно отнести два аспекта:

[507] Джордж П. Флетчер, Иви, 475.

[508] Thomas C. King et al., Ibidem.

Объекты искусственного интеллекта как инструменты: ответственность производителей и пользователей:

Мы разъяснили, что системы ИИ не являются субъектами. Вместо этого их следует рассматривать как инструменты, с помощью которых субъект может совершить преступление. В области медицинских устройств с искусственным интеллектом мы можем выделить два типа правонарушений: те, которые совершаются производителями, и те, которые совершаются пользователями.

Объективная атрибуция – это термин, используемый в Германии для определения общего процесса привлечения лиц к ответственности за причинение вреда или действия других лиц; а также субъективная атрибуция, напротив, относится к отдельному вопросу о критериях привлечения лиц к ответственности за свои действия.

Что касается субъективной атрибуции, то она основана на нормах, отличных от базовых, направленных (не на граждан, а) на судью. Эти правила не создают исключений из основных норм, они лишь оправдывают их нарушение[509].

Производители могут быть привлечены к ответственности за совершение преступлений либо в рамках явной преступности, либо в рамках модели пагубных последствий. В первом случае «значение преступного деяния состоит в том, что оно демонстрирует преступность и расстраивает чувство безопасности сообщества»[510]. Другими словами, наказывается лишь то, что субъект подвергает опасности законный интерес (например, жизнь, или общественное здравоохранение). Эти правонарушения представляют собой формы прямой ответственности, которые могут заключаться в активном или бездействующем поведении (нарушение конкретной установленной законом обязанности действовать) и характеризуются значительным ожиданием порогового значения для активации уголовно-правовой защиты. В этом отношении мы можем выделить:

1.Ответственность за тип производства, когда злоумышленник разрабатывает определенные типы устройств искусственного интеллекта, абсолютно запрещенные законом, поскольку они сопряжены с высоким риском причинения вреда, который не может быть (существенно) снижен за счет соблюдения некоторых мер предосторожности; а также

2. Ответственность за модальность производства, которая относится к областям производства (разрешенным законом), характеризующимся более низким коэффициентом риска, поскольку имеющиеся номологические навыки

---

[509] В этой связи см. Главу Джорджа П. Флетчера «Переосмысление уголовного права» (Oxford / New York: Oxford University Press, 2000), 454-491.
[510] Джордж П. Флетчер, Иви, 420.

позволяют устанавливать меры предосторожности для предотвращения / снижения риска вредных событий[511]. Таким образом, производителей можно привлечь к ответственности за то, что они создали устройства искусственного интеллекта без соблюдения вышеупомянутых правил предосторожности.

Кроме того, они могут быть признаны виновными в преступлении, имеющем вид пагубных последствий, например, в непредумышленном убийстве, поскольку в производственном цикле устройства ИИ они не соблюдают правила предосторожности, упомянутые выше, и из-за этого нарушения, они повлекли за собой фактическое причинение вреда охраняемым законом интересам (жизни человека), например, смерть мужчины/женщины.

Что касается пользователей, а именно врачей, они тоже могут совершать преступления в рамках вышеупомянутых схем. Что касается правонарушений в рамках явной преступности, в сфере SaMD эти формы ответственности могут заключаться в нарушении запрета на простое использование устройств с определенными характеристиками, то есть с уровнем риска, который считается чрезмерным и неприемлемым по закону. Что касается преступлений с опасными последствиями, то врачи могут быть привлечены к ответственности за непредумышленное убийство по причине врачебной халатности. Эти правонарушения могут иметь следующие формы:

1. Прямая ответственность, когда врач совершает активные действия, т.е. он/она использует SaMD, и, как прямое следствие, пациент умирает;

2. Производная ответственность, когда он/она отвечает за так называемую комиссию по бездействию.

Действительно, парадигма совершения бездействия основана на критериях так называемой обязанности предотвратить опасное событие. Обязанность действовать – юридическая, а не просто моральная обязанность – может возникать в соответствии с:

1. Статус («кроме уголовного закона, нарушение которого ставится под сомнение»);[512]

2. Личные отношения, например, между врачом и пациентом;

3. Контракт;

4. Добровольное принятие ухода;

5. Создание риска ответчиком.

---

[511] Франко Брикола, «Responsabilità penale per il tipo e per il modo di produzione», в Scritti di diritto penale, 1, II, ed. Стефано Канестрари и Алессандро Мельчионда (Милан: Джуффре, 1997); Карло Пьергаллини, Danno da prodotto eponsabilità penale: profili dommatici e политико-криминальные (Milano: Giuffrè, 2004), 40-46.
[512] Уэйн Р. Лафэйв и Остин В. Скотт-младший, Иви, 286.

Другими словами, врач может быть привлечен к ответственности за событие, которое должно быть предотвращено, только если – в свете специальной ссылки защиты – в конкретной ситуации он / она может считаться защитником (гарантом) определенного юридического интереса, а именно жизни пациента[513]. Например: врач использовал SaMD; он / она был обязан контролировать это, чтобы предотвратить (насколько это возможно) возникновение пагубных последствий; тем не менее, он/она не справился с этим (либо потому, что он / она абсолютно не контролировал причинно-следственный процесс, вызванный использованием устройства, либо потому, что он/она ошибочно контролировал его, а именно не соблюдал применимые правила). Согласно преобладающему мнению, преступник должен знать факты, указывающие на его обязанность действовать, и судебная практика утверждает, что введение строгой ответственности в случаях бездействия неуместно[514]. Конечно, «иногда может быть обязанность позаботиться о том, чтобы факты, а также обязанность действовать, когда факты известны»[515]. Кроме того, субъект должен быть физически способен выполнять действия, необходимые для предотвращения вредного события[516]. В случае возникновения вредных последствий, когда событие происходит из-за использования систем ИИ может возникнуть проблема со ссылкой на причинно-следственную связь. В настоящее время мы не можем определить этиологические связи в нейронных сетях с точки зрения достоверности. Другими словами, можно утверждать, что система ИИ вызывает определенное событие (например, диагноз) из определенного набора данных (например, некоторые тесты на пациенте). Однако реконструкция каждого промежуточного шага, через который система достигает этого результата (особенно в случаях DL), в настоящее время невозможна.

Тем не менее, с помощью контрфактического анализа судьям нужно только установить, является ли определенное поведение условно важным условием события. Они никогда не достигают дедуктивного результата. В самом деле, их рассуждения почти всегда вероятностны (т. е. рационально правдоподобны) из-за отсутствия объяснительных предварительных условий и использования статистических законов в объяснении натуралистических событий[517]. В этом смысле, как известно, субъект поведение, а именно

---

[513] Этот элемент является общим для нескольких правовых систем. В этой связи можно упомянуть итальянское понятие «posizione di garanzia» или немецкое понятие «Garantenstellung».
[514] Хардинг против Прайса, [1948] 1 KB 695.
[515] Уэйн Р. Лафэйв и Остин В. Скотт-младший, Иви, 290–291.
[516] Уэйн Р. Лафэйв и Остин В. Скотт-младший, Иви, 291 год.
[517] 31 Федерико Стелла, «La nozione penmente rilevante di causa: la condizione needaria», Rivista Italiana di Diritto e Procedura Penale, 4, (1988): 1217.

использование SaMD, должно быть condicio sine qua non для вредного события[518] или того, что, если бы не поведение, событие не произошло бы[519].

По делам о бездействии судья должен:

1. Восстановить пропущенное действие[520], то есть (правильный) контроль устройства, который позволил бы избежать ухудшения состояния здоровья пациента;

2. Реконструировать причинный процесс в том виде, в каком он действительно произошел, т.е. как и почему произошло вредное событие; а также

3. Пояснить – в свете установленного научного закона – могло ли (гипотетическое) поведение субъекта повлиять на причинный процесс, предотвращая вредное событие.

Следует подчеркнуть: стандарт доказывания, выраженный формулой вне всякого разумного сомнения (псевдоним «правило BARD»), возникает из соображения, что «гораздо хуже осудить невиновного человека, чем позволить виновному выйти на свободу»[521]. Следовательно, в этой области необходим установленный закон научного покрытия для доказательства этиологического процесса, а затем и ответственности субъекта. В противном случае обвиняемый врач должен быть признан невиновным.

Для совершения преступления преступник должен соответствовать так называемым требованиям mens rea. В этой связи правонарушения могут быть в основном совершены в свете следующих разновидностей вины[522]:

---

[518] Для целей уголовного права можно утверждать, что существует этиологическая связь между предшествующим (например, - неправильным - диагнозом, полученным с помощью системы искусственного интеллекта) и событием (например, смертью пациента), когда существуют два элемента., а именно: установленный (универсальный или статистический) закон покрытия, в свете которого можно объяснить рассматриваемый причинный процесс; а также поведение агента (т. е. использование системы ИИ) является важным условием во всех возможных (или вероятных) объяснениях.

[519] Американский институт права, Типовой уголовный кодекс, § 2.03 (1) (24 мая 1962 г.).

[520] Джованни Грассо, Il reato omissivo imprieo: La struttura obiettiva della fattispecie (Milano: Giuffrè, 1983), 370-371.

[521] In re Winship, 397 US 358 (1970); Барнс против Соединенных Штатов, 412 US 873 (1973); Карелла против Калифорнии, 491 US 263; Олбрайт против Оливера и др., 510 US 266 (1994); Виктор против Небраски, 511 US 1 (1994); США против Годена, 515 US 506; Спенсер против Кемны, 523 US 1 (1998). Что касается судебной практики Верховного суда Италии, см. Прежде всего: Cassazione Penale, Sezioni Unite, no. 30328 Franzese (2002).

[522] Можно заметить, что различные правовые системы принимают разные решения относительно разновидностей вины. На самом деле это соображение верно лишь отчасти. Напротив, сравнительный анализ показывает, что, несмотря на терминологические различия, существенные сходства часто являются чем-то большим, чем различиями. Конечно, решения редко бывают одинаковыми. Тем не менее, задача современных юристов - живущих в глобализированном мире - состоит в том, чтобы наводить мосты, а не стены, находить точки соприкосновения между различными правовыми традициями, особенно в таких областях, как искусственный интеллект, где преступность (а также ее предотвращение и наказание) больше не касается только одно государство, но требует более сильных механизмов судебного сотрудничества.

С этой точки зрения можно сослаться на правила и принципы, установленные в Римском статуте Международного суда (где применимо). Несомненно, ICC осуществляет свою юрисдикцию в отношении преступлений, отличных от тех, с которыми мы имеем дело, например, преступлений с использованием искусственного интеллекта («AIC») в области здравоохранения. Однако некоторые определения, особенно те, которые касаются так называемой общей части уголовного права, могут представлять собой действительные ссылки. Фактически, составители Статута (большинство из которых были экспертами по сравнительному праву) предприняли попытку сформулировать определения, которые могли бы стать своего рода синтезом различных правовых традиций.

В этой связи, например, можно упомянуть определение mens rea, основанное на элементах намерения и знания, в соответствии со статьей 30: «лицо имеет намерение, если: а) в отношении поведения это лицо средства участвовать в поведении; Что касается последствия, это лицо намеревается вызвать это последствие или осознает, что оно произойдет при обычном ходе событий. «Знание» означает осознание того, что обстоятельства существуют или что последствие наступит при обычном ходе событий».

1. Намерение;

2. Знание;

3. Безрассудство;

4. Халатность.

Среди этих разновидностей вины, безрассудство и небрежность являются наиболее сомнительными в отношении понятия риска (который должен быть существенным и неоправданным)[523]. Действующий субъект – соответственно – сознательно проигнорировал это или должен был знать о нем[524]. Порог существенности и неоправданности риска обусловлен грубым отклонением от стандарта поведения/заботы[525], который законопослушный/разумный человек[526] уважал бы в ситуации субъекта[527].

---

[523] Американский институт права, Типовой уголовный кодекс, § 2.02 (2) (d): «Лицо действует небрежно в отношении существенного элемента правонарушения, когда ему следует осознавать существенный и неоправданный риск того, что материальный элемент существует или будет результатом его поведения. Риск должен быть такого характера и степени, чтобы неспособность актера воспринять его с учетом характера и цели его поведения и известных ему обстоятельств влекла за собой грубое отклонение от стандарта осторожности, который разумный человек соблюдал бы в актерская ситуация ».

[524] В этом отношении мы должны различать три элемента: а) узнаваемость («Erkennbarkeit» в Германии, «riconoscibilità» в Италии) необоснованного/неоправданного риска; б) его предсказуемость («Vorhersehbarkeit» в Германии, «prevedibilità» в Италии); и в) его предотвратимость (Vermeidbarkeit в Германии, evitabilità в Италии).

[525] Понятие «грубое отклонение от стандарта осторожности» выражает то, что обычно понимается как нечто дополнительное, которое отличает преступную (или грубую) халатность от обычной халатности, которая актуальна исключительно в области деликтного права.

Что касается вышеупомянутого стандарта, некоторые правила ухода имеют решающее значение. Что касается производителей, можно сослаться на нормы строгой клинической проверки медицинских устройств с искусственным интеллектом[528]. Вместо этого основным ориентиром являются стандарты ухода за пользователями, то есть врачи, руководства и передовой опыт в области здравоохранения. Однако в обоих случаях судья должен выяснить, было ли в конкретной ситуации нарушенное субъектом правило осторожности направлено на предотвращение вредных событий, подобных тому, что произошло[529].

Новая парадигма

Вышеупомянутая парадигма ответственности (все еще действующая) не позволяет реализовать одновременную защиту невиновных и потерпевших[530]. Другая парадигма может быть теоретически рассмотрена с точки зрения de lege ferenda.

Эти принципы приняты Управлением по контролю за продуктами и лекарствами США (FDA). В этом отношении см. рабочую группу IMDRF SaMD, программное обеспечение как медицинское устройство (SaMD): ключевые определения (9 декабря 2013 г.); Там же, «Программное обеспечение как медицинское устройство»: возможная основа для классификации рисков и соответствующих соображений (18 сентября 2014 г.); Там же. Программное

Аналогичные (хотя и не идентичные) концепции можно найти в правовых системах Германии и Италии: т. е. Понятия «Leichtfertigkeit» и «colpa grave» соответственно.

[526] Уэйн Р. Лафэйв и Остин В. Скотт-младший, Иви, 328: «Таким образом, халатность оформляется с точки зрения объективного (иногда называемого« внешним ») стандарта, а не с точки зрения субъективного стандарта».

[527] В этом отношении см. Также Уэйна Р. Лафэйва и Остина В. Скотта-младшего, Иви, 327-328: «Неоправданный риск» - это выражение, которое принимает во внимание тот факт, что все мы создаем определенный риск для других в повседневной жизни. дела, не неся ответственности за халатность. Таким образом, считается, что критерий разумности в создании риска определяется путем сопоставления величины риска причинения вреда с полезностью поведения субъекта. При таком тесте даже небольшой риск может оказаться необоснованным. Помимо полезности поведения субъекта, еще одним переменным фактором, влияющим на вопрос о том, является ли конкретный риск необоснованным, является степень осведомленности субъекта о фактах, влияющих на риск. Еще одна переменная касается характера и степени вреда, который может быть причинен поведением ответчика, и количества лиц, которым может быть причинен вред ».

[528] Международный форум регулирующих органов в области медицинского оборудования (IMDRF), в котором ВОЗ является официальным наблюдателем в комитете по управлению, в частности, Рабочая группа SaMD, разработала серию документов, чтобы предоставить гармонизированные принципы для принятия отдельными юрисдикциями на основе на собственной нормативно-правовой базе.

[529] В Германии и Италии это понятие понимается, соответственно, как «Risikozusammenhang» и «nesso di rischio». Перевод этих выражений может быть связующим звеном между нарушением обязанности проявлять осторожность (субъектом) и опасным событием, характер которого является нормативным, а не материальным.

[530] 44 Федерико Стелла, Giustizia e modernità: La protezione dell'innocente e la tutela delle vittime (Милан: Джуффре, 2003).

обеспечение как медицинское устройство (SaMD): применение системы менеджмента качества (2 октября 2015 г.); Id., программное обеспечение как медицинское устройство (SaMD): клиническая оценка (22 июня 2017 г.).

В Европе 5 апреля 2017 года Европейский парламент и Совет Европейского Союза приняли Регламент (ЕС) 2017/745 о медицинских устройствах. Это «устанавливает правила, касающиеся размещения на рынке, предоставления на рынок или ввода в эксплуатацию медицинских устройств для использования людьми и аксессуаров для таких устройств в Союзе. Настоящий Регламент также применяется к клиническим исследованиям таких медицинских изделий и принадлежностей, проводимым в Союзе» (статья 1.1). Вышеупомянутое руководство, разработанное для медицинских устройств на международном уровне, также было принято во внимание ЕС, чтобы «способствовать глобальному сближению правил, которое способствует высокому уровню защиты во всем мире, а также для облегчения торговли» (краткое изложение 5). Таким образом, результаты клинических исследований, проведенных в ЕС, будут приниматься в качестве документации за пределами ЕС, а результаты, проведенные за пределами ЕС в соответствии с международными руководящими принципами, будут приниматься в ЕС. В этом отношении правила должны соответствовать самой последней версии Хельсинкской декларации Всемирной медицинской ассоциации (WMA) об этических принципах медицинских исследований с участием людей в качестве субъектов (декларация 64).

В сравнительной правовой панораме хорошим ориентиром может служить американская модель оценки технологических рисков. Он основан на центральной роли государственных органов (например, Управления по контролю за продуктами и лекарствами) и пяти элементах[531]:

1. Агентство предусматривает особые правила предосторожности, которые, например, должны соблюдать компании, занимающиеся производством/использованием медицинских устройств. Эти правила устанавливают стандарты оценки риска, т.е. порог адекватности риска;

2. Принятие этих правил предосторожности является демократически легитимным (т.е. Конгресс утверждает их);

3. Суды проверяют рациональность решений агентств, т. е. апелляционные суды могут признать их недействительными, если они являются

[531] Шейла Джасанофф, «Наука в адвокатуре: право, наука и технологии в Америке» (Кембридж - Массачусетс/Лондон - Англия: издательство Гарвардского университета, 1995), 69–92; Франческо Чентонце, La normalità dei disastri tecnologici: Il проблема congedo dal diritto penale (Milano: Giuffrè, 2004), 400-410.

произвольными, произвольными или не подтвержденными существенными доказательствами[532];

4. Жесткая и превентивная система правоприменения, то есть агентства могут проводить проверки компаний и выносить им судебные запреты;

5. Система обучения и соблюдения нормативных требований, т. е. компании могут либо запросить консультационную помощь агентства в организации адекватного набора мероприятий, способных предотвратить вредные события, либо принять программу добровольной защиты, в свете которой агентство само реализует постоянный анализ сайта по внутренней системе безопасности.

В более широком плане желательна международная гармонизация/сотрудничество в этой области. Всемирная организация здравоохранения (ВОЗ) может установить общие стандарты, которые национальные или, надеюсь, наднациональные агентства, такие как Европейское агентство по лекарственным средствам (EMA), должны (не могут) впоследствии внедрить в более конкретные руководящие принципы для производителей и пользователей.

Что касается санкций, можно предположить многоуровневую систему. Прежде всего, следует различать санкции за ответственность организаций и санкции за ответственность физических лиц.

Что касается первого, можно предположить два уровня:

1. Административные санкции (налагаемые агентством) за незначительные нарушения правил предосторожности, касающихся производства/использования SaMD;

2. Уголовные санкции (налагаемые судами) за серьезные нарушения вышеупомянутых правил предосторожности и, в конечном итоге, за причинение вреда пациентам событий из-за такого нарушения.

Что касается людей, то точка зрения обязательно будет иной: в области, характеризующейся научной неопределенностью, они могут не осознавать, что своими действиями они создают существенный и неоправданный риск. Таким образом, их ответственность должна быть ограничена поведением, охватываемым психологическими коэффициентами намерения и, самое

[532] Закон США об административных процедурах (1946 г.), раздел 10.

большее, безрассудства. За халатные действия в этой области не должны распространяться штрафные санкции[533].

Наконец, следует отметить два соображения. Во-первых, независимо от того, является ли обвиняемый организацией или физическим лицом, правило доказывания и вынесения приговора в уголовных процессах выражается формулой вне всякого разумного сомнения. Затем, в случаях, когда прокуроры не могут представить достаточные доказательства, чтобы удовлетворить вышеупомянутый стандарт (либо потому, что они не находят его, либо потому, что – особенно в отношении ответственности отдельных лиц – его не существует), потерпевшие могут пойти по пути деликтного права, чтобы получить справедливую компенсацию за понесенный ущерб. В этом отношении мнение тех, кто теоретизирует определения уголовной ответственности без требования о вине, не может быть принято, и mens rea настолько важна для права государства налагать санкции на лиц, лишающих их свободы, что мы не можем просто отказаться от нее только из-за трудностей доказывая это.

Выводы

Подводя итог, мы увидели, что приложения искусственного интеллекта в здравоохранении влекут за собой как преимущества, так и риски, которые необходимо сбалансировать. Поиск равновесия между ними требует рассмотрения не только медицины, но также этики и права.

В частности, заслуживает внимания защита прав человека. Среди них, в области уголовного права, следует подчеркнуть взаимосвязь, существующую между, с одной стороны, принципами законности (nullum crimen sine lege) и вины (nullum crimen sine culpa), а с другой стороны, их процессуальная часть, а именно презумпция невиновности и правило BARD (правило, относящееся как к допущению и оценке доказательств, так и к приговору о виновности подсудимого). С точки зрения обвиняемых, соблюдение этих принципов имеет решающее значение, чтобы гарантировать фундаментальное право на справедливое судебное разбирательство. Тем не менее, пациенты-жертвы заслуживают правосудия в случае ущерба, причиненного ошибками в

[533] Томас К. Кинг и др., Иви, 95: «Что касается порога знаний, то в некоторых случаях mens rea может вообще отсутствовать. Потенциальное отсутствие основанных на знаниях людей объясняется тем фактом, что даже если предполагается, что AA [искусственный агент] может выполнять повторное действие автономно, сложность программирования AA делает возможным, что проектировщик, разработчик, или развертывающее лицо (то есть агент-человек) не будет ни знать, ни предсказать преступное действие или бездействие AA. Подразумевается, что сложность ИИ является отличным стимулом для агентов-людей избегать выяснения того, что именно делает система машинного обучения [машинного обучения], поскольку чем меньше агенты-люди знают, тем больше они смогут отрицать ответственность за обе стороны. эти причины ».

применении методов искусственного интеллекта в их клинической практике. ситуация. Мы видели, как может быть достигнута одновременная защита невиновных и жертв. В первую очередь, не следует путать ответственность производителей и врачей. Первые могут быть признаны виновными в совершении правонарушений либо в рамках явной преступной деятельности (т.е. Они нарушают абсолютный запрет на производство определенных типов устройств, или они разрабатывают устройства без соблюдения применимых правил предосторожности), либо в рамках модели нанесения вреда последствия (поскольку нарушение мер предосторожности этиологически связано со смертью мужчины/женщины). Напротив, дело об ответственности врачей – это, по сути, дело врачебной халатности. Затем, с другой точки зрения, следует различать случаи ответственности физических и юридических лиц, учитывая, что несколько законодательств могут по-разному применяться к каждому из них. Наконец, с точки зрения de lege ferenda, мы увидели, что новую парадигму можно теоретизировать. Он основан на американской модели оценки рисков и включает интеграцию мер уголовного, гражданского и административного права. Я думаю, что эта модель могла бы гарантировать равновесие между основными правами обвиняемого (справедливое судебное разбирательство) и потерпевших (компенсация понесенного ущерба).

Ссылки

Боден, Маргарет А. Искусственный интеллект. Очень краткое введение. Oxford: Oxford University Press, 2018 (итальянский перевод, L'intelligenza artificiale. Болонья: Il Mulino, 2019).

Брикола, Франко. «Responsabilità penale per il tipo e per il modo di produzione». В Scritti di diritto penale, 1, II, под редакцией Стефано Канестрари и Алессандро Мельчионда. Милан: Джуффре, 1997.

Чентонце, Франческо. La normalità dei disastri tecnologici: Il проблема congedo dal diritto penale. Милан: Джуффре, 2004.

Флетчер, Джордж П. Переосмысление уголовного права. Оксфорд/Нью-Йорк: Издательство Оксфордского университета, 2000.

Грассо, Джованни. Il reato omissivo imprieo: La struttura obiettiva della fattispecie. Милан: Джуффре, 1983.

Грассо, Джованни. «La protezione dei diritti fondamentali nella Costituzione per l'Europa e il diritto penale: spunti di riflessione critica». в Lezioni di diritto

penale europeo, под редакцией Джованни Грассо и Розарии Сикурелла. Милан: Джуффре, 2007.

Ясанов, Шейла. Наука в адвокатуре: право, наука и технологии в Америке. Кембридж - Массачусетс / Лондон - Англия: Издательство Гарвардского университета, 1995.

Лафэйв, Уэйн Р. и Остин В. Скотт-младший. Материальное уголовное право. Том 1. Сент-Пол - Миннесота: West Publishing Co., 1986.

Пьергаллини, Карло. Danno da prodotto e responsabilità penale: profili dommatici e политико-криминальный. Милан: Джуффре, 2004.

Стелла, Федерико. Giustizia e modernità: La protezione dell'innocente e la tutela delle vittime. Милан: Джуффре, 2003.

Касонато, Карло. «Potenzialità e sfide dell'intelligenza artificiale». BioLaw Journal, 1 (2019): 177-182.

Флориди, Лучано, Джош Коулс, Моника Бельтраметти, Раджа Чатила, Патрис Чазеран, Вирджиния Дигнум, Кристоф Лютдж и другие. «AI4People - этические рамки для хорошего общества искусственного интеллекта: возможности, риски, принципы и рекомендации». Умы и машины 28, 4 (2018): 689-707. https://doi.org/10.1007/s11023-018-9482-5.

48 Джованни Грассо, «La protezione dei diritti fondamentali nella Costituzione per l'Europa e il diritto penale: spunti di riflessione crisica», в Lezioni di diritto penale europeo, ed. Джованни Грассо и Розария Сикурелла (Милан: Giuffrè, 2007), 656-659-58

Флориди, Лучано. «Раскалывающая сила цифровых технологий и ее последствия». Филос. Technol. 30, (2017): 123-129. https://doi.org/10.1007/s13347-017-0259-1.

Халлеви, Габриэль. «Уголовная ответственность субъектов искусственного интеллекта - от научной фантастики до правового социального контроля». Akron Intellectual Property Journal 4, 2, статья 1 (2010): 186. http://ideaexchange.uakron.edu/akronintellectualproperty/vol4/iss2/1.

Цзян, Фэй, Юн Цзян, Хуэй Чжи, И Донг, Хао Ли, Суфэн Ма, Илун Ван, Цян Донг, Хайпэн Шен и Юнцзюнь Ван. «Искусственный интеллект в здравоохранении: прошлое, настоящее и будущее». Инсульт и сосудистая неврология 2, 4 (2017): 230. http://dx.doi.org/10.1136/svn-2017-000101.

Кинг, Томас К., Никита Аггарвал, Мариаросария Таддео и Лучано Флориди. «Преступление с применением искусственного интеллекта:

междисциплинарный анализ прогнозируемых угроз и решений». Sci. Англ. Этика 26, (2020): 90-91. https://doi.org/10.1007/s11948-018-00081-0.

Ледли, Роберт С. и Ли Б. Вожделение. «Обоснование основ медицинской диагностики; символическая логика, теория вероятностей и ценностей помогают нам понять, как рассуждают врачи ». Science 130, 3366 (3 июля 1959 г.);

Маккарти, Джон, Марвин Л. Мински, Натаниэль Рочестер и Клод Э. Шеннон. «Предложение для Дартмутского летнего исследовательского проекта по искусственному интеллекту; 31 августа 1955 года ». AI Magazine 27, 4 (2006): 12. https://doi.org/10.1609/aimag.v27i4.1904.

Пак, Янг-Сеук и Сован Лек. «Искусственные нейронные сети: многослойный персептрон для экологического моделирования». События в экологическом моделировании, 28 (2016): 124. https://doi.org/10.1016/B978-0-444-63623-2.00007-4.

Ригби, Майкл Дж. «Этические аспекты использования искусственного интеллекта в здравоохранении». AMA J Ethics 21, 2 (2019): 121-124. https://journalofethics.ama-assn.org/article/ethical-dimensions-using-artificial-intelligence-health-care/2019-02.

Сария, Сучи, Атул Бютте и Азиз Шейх. «Лучшая медицина через машинное обучение: что реально, а что искусственно?». PloS Med 15, 12 (2018): 1. https://doi.org/10.1371/journal.pmed.1002721.

Семигран, Ханна Л., Дэвид М. Левин, Шантану Нунди и Атеев Мехротра. «Сравнение точности диагностики врача и компьютера». JAMA Internal Medicine 176, 12 (2016): 1860-1861. https://jamanetwork.com/journals/jamainternalmedicine/fullarticle/2565684.

Шортлифф, Эдвард Х. и Мартин Дж. Сепульведа. «Поддержка принятия клинических решений в эпоху искусственного интеллекта». JAMA 320, 21 (4 декабря 2018 г.): 2199.

Стелла, Федерико. «La nozione Penalmente rilevante di causa: la condizione needaria». Rivista Italiana di Diritto e Procedura Penale, 4, (1988): 1217-1268.

Олбрайт против Оливера и др., 510 US 266 (1994).

Барнс против Соединенных Штатов, 412 US 873 (1973).

Карелла против Калифорнии, 491 US 263.

Cassazione Penale, Sezioni Unite. нет. 30328 Franzese (2002).

Комиссия ЕС. Искусственный интеллект для Европы, Сообщение Комиссии Европейскому парламенту, Европейскому совету, Совету,

Европейскому экономическому и социальному комитету и Комитету регионов, 2 (25 апреля 2018 г.).

Группа экспертов ЕС высокого уровня по ИИ. Этические принципы надежного ИИ, 4 (8 апреля 2019 г.).

https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Хардинг против Прайса, [1948], 1 KB 695.

IMDRF SaMD Рабочая группа. «Программное обеспечение как медицинское устройство»: возможные рамки для классификации рисков и соответствующие соображения (18 сентября 2014 г.).

IMDRF SaMD Рабочая группа. Программное обеспечение как медицинское устройство (SaMD): применение системы менеджмента качества (2 октября 2015 г.).

IMDRF SaMD Рабочая группа. Программное обеспечение как медицинское устройство (SaMD): клиническая оценка (22 июня 2017 г.).

IMDRF SaMD Рабочая группа. Программное обеспечение как медицинское устройство (SaMD): ключевые определения (9 декабря 2013 г.).

In re Winship, 397 US 358 (1970).

Спенсер против Кемны, 523 US 1 (1998).

Американский юридический институт. Типовой уголовный кодекс, § 2.03 (1) (24 мая 1962 г.).

Европейский парламент и Совет Европейского Союза. Регламент (ЕС) 2017/745 о медицинских изделиях (5 апреля 2017 г.).

Закон США об административных процедурах (1946 г.).

США против Годена, 515 US 506.

Виктор против Небраски, 511 US 1 (1994).

Искусственный интеллект: deepfakes как пример вызовов ии системам уголовного правосудия

Хин-Ян Лю * и Эндрю Мазибрада **[534]

[534] 1 * Хин-Ян Лю - доцент и координатор исследовательской группы по искусственному интеллекту и нарушениям законодательства юридического факультета Копенгагенского университета. Почта: hin-

В этой статье делается попытка предоставить единую концептуальную основу для интерпретации опасностей и перспектив применения искусственного интеллекта (ИИ) в системах уголовного правосудия. Как платформенные технологии, которые поддерживают множество потенциальных приложений, влияние систем искусственного интеллекта на уголовное правосудие будет усиливаться, расходиться и одновременно. Объединяющая структура будет способствовать целостному пониманию того, почему системы искусственного интеллекта могут дестабилизировать системы уголовного правосудия, и предлагать соответствующие ответные меры в зависимости от типа уголовно-правового нарушения, лежащего в его основе. Мы разрабатываем эту теоретическую основу, анализируя проблемы, создаваемые генеративной технологией «глубокого подделки», в контексте системы уголовного правосудия в Англии и Уэльсе. Ценность этой структуры состоит в том, что она заставляет нас задавать вопросы о ранее существовавших нормативных и процедурных ответах таким образом, чтобы выявлять будущие проблемы, вместо ограниченных обсуждений применения и адаптируемости существующих систем, чего нет.

Ключевые слова: Deep-fake, изобретенный аффорданс, невидимый аффорданс, неиспользованный аффорданс, искусственный интеллект и система уголовного правосудия.

Вступление

Основной вопрос, который мы здесь рассматриваем, заключается не в том, что ИИ сделает с нами или что мы можем сделать друг с другом с помощью ИИ 1, а скорее в том, какие эффекты ИИ будет оказывать с точки зрения эпистемологических сомнений и неопределенности в системах уголовного правосудия. Это имеет широкие последствия для: получения доказательств в уголовных процессах; создание возможностей для совершения новых разновидностей категорий преступлений, таких как мошенничество, шантаж или вмешательство в выборы; выявление фундаментальных недостатков в юридических процессах и принципах; и изменение социально-политического ландшафта таким образом, чтобы отдавать предпочтение организованным, технологическим специалистам или богатым, которые

---

yan.liu@jur.ku.dk
** Эндрю Мазибрада - научный сотрудник Центра междисциплинарных исследований права и исследовательской группы по искусственному интеллекту и нарушениям законодательства юридического факультета Копенгагенского университета. Ранее работал в Коллегии адвокатов по уголовным делам Англии и Уэльса и в Королевской прокуратуре Лондона. Почта: andrew.mazibrada@jur.ku.dk
Джек М. Балкин, «Путь закона о робототехнике», California Law Review Circuit 6 (июнь 2015 г.): 45–60.

занимаются преступной деятельностью. Короче говоря, эти эффекты демонстрируют, что ИИ вмешивается в процессы, происходящие как в инфраструктурах, так и в действующих лицах, которые привыкли к их существованию и способам работы, так что теперь технология занимает невидимый слой, который едва осознается до тех пор, пока не перестает работать. эффективно функционировать[535]. Это делает нас уязвимыми для манипуляций с помощью этой технологии и, для конкретных целей нашего анализа, проявляется, среди прочего, в предполагаемой достоверности аудиовизуальных записей[536].

Финансовые средства: концептуальная основа

Концепция «аффорданса» была введена Джеймсом Гибсоном для одновременной ссылки на все возможности действия, доступные агенту в его среде: «аффорданс среды – это то, что оно предлагает животному, то, что оно обеспечивает или предоставляет, либо во благо, либо во благо. ill'[537]. Понятие аффордансов было впоследствии адаптировано и популяризировано Доном Норманом для обозначения воспринимаемых действий; т.е, которые агенты рассматривают как возможности[538]. Построенная на этих корнях, социокультурная модель для теории аффорданса[539] представляет собой дальнейшее развитие путем структурирования взаимодействий между аффордансами «что можно сделать»; преднамеренность «что было бы сделано»; и нормативность «что делать». Таким образом, он помещает концепцию аффордансов в более широкий контекст, который влияет или структурирует возможности и ограничения, налагаемые на агента окружающей средой (в расширенном и контекстном смыслах, которые также учитывают нормативные и социальные аспекты среды, а не просто в физико-географическом смысле)[540].

---

[535] 2 Дэниел Сассер, «Невидимое влияние: искусственный интеллект и этика архитектур выбора», на конференции AAAI / ACM по ИИ, этике и обществу (AIES '19), (Нью-Йорк, Нью-Йорк: ACM, 2019). https://doi.org/10.1145/3306618.3314286. См. Также развивающуюся область постфеноменологии и, в частности, Дэниела Сассера, «Прозрачные медиа и развитие цифровых привычек», в книге «Постфеноменология и медиа: эссе о взаимоотношениях человека, технологий и мира», изд. Йони Ван Ден Эеде и др. (Lanham: Lexington Books, 2017), 27–44, и Дайан Мишельфельдер, «Постфеноменология глазами в будущее», в Postphenomenological Investigations: Essays on Human-Technology Relations, eds. Роберт Розенбергер и Питер-Поль Вербик (Lanham: Lexington Books, 2015), 237–46.

[536] 3 В этой статье мы используем «правдивость» для обозначения истинности содержания записи, а именно, действительно ли то, что она представляет, имело место в представленной манере (звуковой или визуальной).

[537] 4 Джеймс Дж. Гибсон, Экологический подход к визуальному восприятию (Хиллсдейл, штат Нью-Джерси: Эрлбаум, 1986) 127.

[538] 5 Дональд Норман, Дизайн повседневных вещей (Кембридж, Массачусетс: MIT Press, 2016).

[539] 6 Влад П. Главяну, «Что можно сделать с яйцом? Творчество, материальные объекты и теория средств », Журнал творческого поведения 46, № 3, (2012): 192–208.

[540] 7 В оригинальной формулировке Джеймса Гибсона.

Мы принимаем и адаптируем эту структуру для определения конкретных типов возможностей на пересечении этих категорий, которые, как мы предполагаем, помогут в исследованиях и разработке политики в отношении того, как системы ИИ будут влиять, искажать или нарушать работу систем уголовного правосудия. Эти пересечения выявляют «выдуманные возможности», при которых отсутствие (технологических) возможностей больше не является ограничивающим фактором для поведения; «невоспринимаемые аффордансы», когда отсутствие распознавания возможностей для действий подкрепляет ограничение в поведении; и «неиспользованные аффордансы», когда отсутствие действий или развертывания ограничивает возможное поведение541. Таким образом, предлагаемая нами модель предлагает дополнительные нюансы в выявлении и изучении качества и природы действующего типа аффорданса. Это, в свою очередь, позволяет нам уточнить наш анализ сдвигов и возмущений социотехнического ландшафта, лежащих в основе уголовно-правового нарушения, которое ИИ создает для системы уголовного правосудия.

В большинстве современных исследований системы искусственного интеллекта рассматриваются либо как объект регулирования (системы искусственного интеллекта должны подлежать регулированию), либо как с точки зрения возможностей регулирования (системы искусственного интеллекта могут вытеснить или исказить современную конфигурацию модальностей регулирования). Это помещает большую часть современной литературы в категорию «изобретенных аффордансов», где, возможно, ничего нового не происходит. Например, ИИ был (спорно), развернутым в принятии риска-оценки для судебных решений, приговоров и поворот к предсказательной охраняя strategies. В таких условиях, однако, системы ИИ являются лишь инструментами, развернутые в процессы, которые уже существуют, в результате воздействия это можно считать количественным (усугубляющим текущие проблемы), а не обязательно качественным (введение новых форм проблем).

Структура, которую мы изложили в этой статье, предлагает и исследует ещё две области, в которых система уголовного правосудия может быть дестабилизирована. Мы рассматриваем ситуации, когда системы ИИ делают возможными новые типы поведения, но эти возможности еще не были признаны («невоспринимаемые» аффордансы); и где системы ИИ создают новые типы поведения, которые являются признанными возможностями, но которые еще не были реализованы («неиспользованные» аффордансы). Поскольку эти способности являются скрытыми и поскольку распознавание и

---

[541] 8 Хин-Ян Лю, Маттис Маас, Джон Данахер, Луиза Скарселла, Микаэла Лексер и Леонард Ван Ромпей, «Искусственный интеллект и нарушение законодательства: новая модель анализа», Право, инновации и технологии 12, т. 2 (2020).

реализация препятствуют последовательным формам поведения, мы утверждаем, что точную природу этих эффектов второго порядка труднее распознать и предсказать, и в результате они значительно более разрушительны. Признание и реализация происходят непостоянно и внезапно, потому что они зависят от проницательности и творческих способов мышления, и поэтому прогресс труднее контролировать, анализировать и оценивать. Эти характеристики имеют далеко идущие последствия для систем уголовного правосудия, потому что разрушительные воздействия в первую очередь не проистекают из того, что представляет собой новая технология, или из того, что она может делать: скорее, такие воздействия полностью зависят от творческого осознания того, как можно использовать такую технологию, и как эта технология фактически развертывается. Чтобы продемонстрировать структуру аффордансов для целей данной статьи, мы будем использовать ИИ, применяемый в качестве генеративных состязательных сетей (GAN) для облегчения «глубоких подделок»[542]. Кроме того, это непредвиденное обстоятельство распространяется на то, как аффордансы, открываемые новой технологией, сочетаются с возможности, уже существующие в мире, а также потенциальные возможности, представленные другими новыми и появляющимися технологиями. Чтобы продемонстрировать это, мы используем повсеместное распространение смартфонов, обладающих возможностями аудиовизуальной записи, хранения и распространения.

Взятые по отдельности и по причинам, которые мы исследуем ниже, мы предполагаем, что технологическая способность манипулировать или фальсифицировать[543] аудио и визуальным материалом убедительным образом –

---

[542] В задачу данной статьи не входит обсуждение способов создания глубоких фейков, их исторического развития или бесчисленных угроз, которые они несут вне контекста уголовного правосудия. Для общего обсуждения глубоких фейков и введения во многие проблемы, связанные с ними, см., Например, Роберт Чесни и Даниэль Ситрон, «Глубокие фейки: надвигающийся вызов конфиденциальности, демократии и национальной безопасности». California Law Review 107, no. 6 (1 декабря 2019 г.): 1753; Роберт Чесни и Даниэль Китс Ситрон, «Разложение истины в стиле 21-го века: глубокие подделки и вызов конфиденциальности, свободе выражения мнений и национальной безопасности», Maryland Law Review 78, вып. 4 (2019): 882-891; Мэри Энн Фрэнкс и Ари Эзра Уолдман, «Секс, ложь и видеокассеты: подделки и заблуждения о свободе слова», Maryland Law Review 78, вып. 4 (2019): 892-898; и Холли Кэтлин Холл, «Глубокие фальшивые видео: когда видеть - не верить», Журнал права и технологий Католического университета 27, вып. 1 (осень 2018 г.): 51-76. Для недавнего анализа текущего состояния коммодификации дип-фейков см. Роберт Волкерт и Генри Аджер, «Анализ коммодитизации дип-фейков». Журнал законодательства и государственной политики Нью-Йоркского университета, 27 февраля 2020 г., https://nyujlpp.org/quorum/volkert-ajder-analyzing-the-commoditization-of-deep-fakes/ (по состоянию на 28 февраля 2020 г.) и Генри Эйдер, Джорджио Патрини, Франческо Кавалли и Лоуренс Каллен, «Состояние глубоких подделок: ландшафт, угрозы и влияние». Deeptrace Labs, сентябрь 2019 г.

[543] В этой статье мы используем термин «манипуляция» для обозначения преднамеренного изменения ранее существовавшей записи и «фабрикация» для обозначения создания записи с нуля с использованием несвязанного ранее существовавшего материала, который имеет мало или вообще не имеет отношения к рассматриваемые факты. Манипуляции включают, например, так называемые «мелкие подделки» или «дешевые подделки», такие как печально известное видео с участием конгрессмена США Нэнси Пелоси, которое было замедлено, чтобы спикер палаты представителей выглядел в состоянии алкогольного опьянения, на котором можно увидеть, например,, Роберт Чесни, Даниэль Ситрон и Квинта Юречич, «Это видео Пелоси: что делать с 'Cheapfakes' в 2020 году», Lawfare (29 мая 2019 г.), https://www.lawfareblog.com/about-pelosi-video - Что-делать-о-дешевых-подделках-2020.

это то, что уголовные процессы смогут в относительно короткие сроки приспособить. Когда глубокие подделки сочетаются с повсеместной возможностью записи, хранения и распространения аудио- и визуальных материалов, перед системами уголовного правосудия в целом возникают более серьезные и фундаментальные проблемы.

Генеративные состязательные сети (GAN) и улики по уголовным делам

Мы начинаем с изучения потенциального воздействия глубоко фальшивых манипуляций и фальсификации аудиовизуальных материалов, предлагаемых в качестве доказательств в системе уголовного правосудия Англии и Уэльса (далее: английская система). Мы делаем это потому, что наиболее очевидный эффект феномена глубокой подделки в данном контексте заключается в получении доказательств в уголовном процессе[544]. Вопросы допустимости в отношении аудиовизуальных доказательств иллюстрируют прямые проблемы, создаваемые манипуляциями и фабрикацией глубоко подделок, и способ, с помощью которого суды могут изначально бороться, чтобы адекватно классифицировать это явление и отреагировать на него. Однако, хотя и проблематично, глубоко фальшивые доказательства сами по себе не являются основной проблемой. Мы предполагаем, что ситуация более сложная, и предлагаемая нами структура аффордансов раскрывает эту сложность.

Вначале нам нужно сделать два наблюдения, которые определяют основу нашего анализа. Во-первых, выявление манипуляций или фальсификаций, осуществленных GAN, с любой степенью подлинной уверенности, не говоря уже о том, чтобы доказать это преступным стандартам и возложить на них ответственность, в настоящее время невозможно[545] с помощью технических

---

[544] Хотя это может показаться очевидным, на удивление мало обсуждений в этой области, особенно доктринально, со стороны ученых-юристов. См., Однако, Центр этики данных и инноваций (CDEI). «Дипфейки и аудиовизуальная дезинформация». (Сентябрь 2019 г.), 10–14 (Центр этики данных и инноваций является экспертным комитетом Департамента цифровых технологий, культуры, СМИ и спорта Соединенного Королевства). См. Также Джефф Уорд, «10 вещей, которые судьи должны знать об ИИ». Судебная власть 130, нет. 1 (2019) 12-18; Мари-Элен Марас и Алекс Александру. «Определение подлинности видеодоказательств в эпоху искусственного интеллекта и после видео Deepfake». Международный журнал доказательств и доказательств 23, № 3 (2019): 255–262; Ребекка Дж. Гамильтон. «Новые технологии в международных уголовных расследованиях». Материалы ежегодного собрания ASIL 112 (2018): 131–33; и Ребекка Дж. Гамильтон. «Доказательства, созданные пользователями». Колумбийский журнал транснационального права 57, № 1 (2018) Американский университет, Исследовательский доклад WCL № 2018-11.

[545] Там же, сноска 11 и публикация, сноска 18. Хотя сейчас ведется работа по разработке и тестированию систем искусственного интеллекта, способных обнаруживать глубокие подделки (см., Например, Джей Питерс, «Головоломка от Alphabet представляет инструмент, который помогает журналистам обнаруживать глубокие подделки»). и манипулировали изображениями », The Verge, 4 февраля 2020 г., https://www.theverge.com/2020/2/4/21122778/alphabet-jigsaw-assembler-tool-news-journalists-deep-fakes-images) там вызывает серьезную озабоченность по поводу того, что машинное обучение (ML) всегда будет опережать

средств. Такое доказательство, конечно, может быть возможным с помощью других подтверждающих средств, например, с помощью контекстуальных доказательств или свидетельских показаний, и это мы подробно рассмотрим ниже. Во-вторых, обработка и изготовление аудио и видео не являются чем-то новым как таковые – кинопроизводство использует итерации этого с тех пор, как существует кино, что приводит к созданию сложных компьютерных игр и фильмов с большим количеством эффектов, таких как «Аватар» Джеймса Кэмерона.

Сдвиг парадигмы, который, как мы предполагаем, происходит сейчас, включает в себя размытые социальные и технологические контексты, которые не только начинают снижать порог для участия в таких манипуляциях и фабрикациях, но и делают аудиовизуальные материалы повсеместными и более легкими в использовании[546]. Это «выдуманные возможности», когда отсутствие технологических возможностей, которое когда-то было ограничивающим фактором поведения, больше не существует. Однако если дип-фейки существовали в вакууме, даже снижение таких пороговых значений для входа не вызвало бы особых поводов для беспокойства суды могли адаптироваться к небольшому количеству дел, в которых предположительно имели место манипуляции или фабрикация с помощью технологии GAN. Серьезность эффекта раскрывается только в контексте повсеместности.

Вопрос о доказательствах открывает перед уголовным судом два ключевых потенциала. Первый заключается в способности любой стороны, особенно обвиняемой, поставить под сомнение, независимо от истинности дела, достоверность доказательств, которые ранее были бы приняты[547] как фактические на первый взгляд. Во-вторых, это способность любой стороны судебного разбирательства манипулировать доказательствами или сфабриковать их, причем потенциально безнаказанно. И то и другое действительно возможно благодаря повсеместному распространению. Даже сейчас, если обвиняемые возражали против правдивости аудиовизуальных доказательств без подтверждающих доказательств, они обычно отклонялись бы в дисциплинарном порядке. В ближайшие годы ситуация, скорее всего,

---

любые созданные алгоритмы обнаружения (см. Джеймс Винсент, «Алгоритмов обнаружения глубоких подделок никогда не будет достаточно», The Verge, 27 июня 2019 г., https: //www.theverge .com / 2019/6/27/18715235 / deep-fakes-detection-ai-algorithmms-precision-will-they-ever-work). Об асимметрии баланса «нападение / защита» в ИИ см. Бен Гарфинкель и Аллан Дефо, «Как изменяется баланс между атакой и защитой?», Журнал стратегических исследований, 42, том 26, (2019): 736-763, DOI: 10.1080 / 01402390.2019.1631810.

[546] При использовании слова «развертывание» мы имеем в виду все средства работы с записью после того, как она была сделана: сохранение, хранение, использование, отображение и совместное использование. Все стало дешевле
и проще, и обмен потенциально может охватить более широкую целевую аудиторию, ранее недоступную или труднодоступную.

[547] Обычно в виде опровержимой презумпции, о которой много говорится в этой статье.

изменится, поскольку такое обвинение становится все более обоснованным. Опять же, это «придуманные» аффордансы: обе эти состязательные тактики судебной экспертизы существовали до глубокой подделки – обвиняемые в уголовных процессах давно заявляли, что они подбрасывают доказательства или что свидетель лгал под присягой. В некоторой степени то же самое можно сказать и о сфабрикованных доказательствах, таких как предъявление поддельного документа в качестве доказательства. Системы уголовного правосудия построены вокруг решения проблемы такого поведения путем взвешивания и допустимости доказательств или, в частности, путем определения правонарушений, как лжесвидетельство[548]. Таким образом, здесь происходит двойная смена парадигмы. Во-первых, обработанный или сфабрикованный материал станет более доступным и легко используемым, и вскоре может достигнуть точки, когда обнаружение подделки станет навсегда невозможным[549] – визуальные подсказки могут фактически исчезнуть, а технические подсказки могут быть вынуждены прибегнуть к вероятностным утверждениям, которые не адекватно соответствуют современной доказательной парадигме. Во-вторых, то, что могло быть дискретной, сдерживаемой проблемой, усиливается или иным образом трансформируется в различные типы проблем в контексте повсеместности.

В английской системе основное правило доказывания заключается в том, что с учетом любых применимых правил исключения или судебного усмотрения все доказательства, которые в достаточной мере относятся к рассматриваемым фактам, являются допустимыми, а все доказательства, которые не имеют отношения к делу или недостаточно значимы, должны быть исключены. Свидетельство, имеющее отношение к делу, может быть исключено, если никакое разумное жюри, должным образом направленное на его недостатки, не могло придать ему никакого значения[550]. При работе с аудио

---

[548] В этой короткой статье важно отметить, что некоторые аргументы выходят за рамки ее рассмотрения. Однако это не означает, что они не важны. По аналогии, ведутся серьезные споры о возможности криминализации создания глубоких подделок. Это создает серьезные, потенциально непреодолимые проблемы. Во-первых, программные приложения, допускающие глубокие подделки, часто кодируются множеством сторон, часто на форумах, где ценится и защищается анонимность, почти всегда из нескольких юрисдикций. В отношении свободы выражения мнения также приводятся аргументы в пользу прав человека. Здесь делается попытка продемонстрировать отсутствие четких решений, как это часто бывало в прошлом, когда речь идет о криминализации нового поведения. Подобные аргументы станут предметом дальнейших исследований авторов данной статьи.

[549] Там же, сноска 11. Важная работа эксперта по изображениям Дартмутского колледжа Хани Фарида в области криминалистики изображений включает в себя обнаружение дипфейков в этой области: Хани Фарид. «Судебная экспертиза изображений». Ежегодный обзор Vision Science 5, номер 1 (2019), 549-573 и Шрути Агарвал, Хани Фарид, Юмин Гу, Минмин Хе, Коки Нагано и Хао Ли. «Защита мировых лидеров от глубоких подделок». В материалах конференции IEEE по компьютерному зрению и семинарам по распознаванию образов (2019): 38–45. В контексте Новой Зеландии и с использованием конкретной доктринальной правовой методологии см. Curtis Barnes and Tom Barraclough. «Начало восприятия: подготовка к дипфейкам и синтетическим медиа завтрашнего дня». Фонд права Новой Зеландии, 21 мая 2019 г., https://www.brainbox.institute/report.

[550] Для отличного резюме см., Например, Дэвид Ормерод, QC и Дэвид Перри, QC, Blackstone's Criminal Practice 2019, (Oxford: OUP 2019), F1.11, где одним из примеров является Robinson [2006] 1 Cr App R 13 (at 221), дело

и видеодоказательствами допустимость и актуальность основываются на неявной презумпции правдивости. Эта позиция ставит под сомнение взаимосвязь между копиями и оригинальной записью (которая в судебной практике проблематично называется «аутентичностью»), игнорируя или иным образом недооценивая возможность того, что оригинал сам по себе является сфабрикованным. Это свидетельствует о влиянии неосознанных и неиспользованных возможностей для уголовного правосудия – оно не учитывает возросшие комбинированные возможности и использование смартфонов и GAN для снижения барьеров для доступа для манипулирования и изготовления аудиовизуальных доказательств.

Об этом недостатке свидетельствует давно установившаяся презумпция того, что механические и другие инструменты аналогичного типа, которые обычно находятся в рабочем состоянии, находились в рабочем состоянии во время их использования[551]. Сторона, против которой действует презумпция, несет бремя доказывания привести доказательства обратного. Если эта относительно низкая планка будет пересечена и правдивость записи будет поставлена под вопрос, возникнут фундаментальные вопросы относительно допустимости и веса, и простых ответов не будет. Перекрестный допрос долгое время был одним из основных традиционных средств тестирования и оценки оспариваемых доказательств, но если создатель записи недоступен или неизвестен, что правдоподобно в сегодняшней глобальной среде социальных сетей, это может быть невозможно. Косвенные доказательства также влияют на вес и приемлемость, и суды могут быть все чаще вынуждены больше полагаться на этот тип доказательств[552]. Проблемы возникают, когда других таких доказательств мало или совсем нет и когда манипуляции или фабрикация не предусмотрены непродуманным законодательством. В качестве примера в этой статье позже рассматриваются правонарушения, с которыми насилие в отношении женщин и девочек.

о доказательствах распознавания голоса. Доказательства имеют значение, «если они являются логически доказательными или опровергающими в отношении какого-либо вопроса, требующего доказательства». DPP v Kilbourne [1973] AC 729, at p. 756 за лорд Саймон Глейсдейл.

[551] В деле Tingle Jacobs & Co. против Кеннеди [1964] 1 All ER 888, как сказал лорд Деннинг M.P. (на стр. 639), «когда у вас есть такое устройство, настроенное для публичного использования в активной работе ... будь то он находится в надлежащем рабочем состоянии, если нет доказательств противного ». Кроме того, см. Перри и Ормерод, Криминальная практика Blackstone 2019, F3.59.

[552] Само по себе это не обязательно проблематично, и из этого не обязательно следует, что косвенные доказательства будут иметь меньший вес, чем прямые доказательства. Тем не менее, косвенные свидетельства «действуют кумулятивно, в геометрической прогрессии, исключая другие возможности» (DPP v Kilbourne [1973] AC 729 per Lord Simon, 758). Некоторые считают это веревкой, которая сама по себе слабее, чем другие доказательства, к которым нужно привязаться. Несмотря на то, что косвенные доказательства могут иногда быть доказательными, они всегда должны подвергаться тщательной проверке, поскольку фабрикация всегда является актуальной проблемой: «Также необходимо, прежде чем делать вывод о виновности обвиняемого на основе косвенных доказательств, убедиться, что нет других доказательств. -существующие обстоятельства, которые могут ослабить или разрушить вывод». (Тепер против Королевы [1952] AC 480, лорд Норманд, 489).

(VAWG) «Стратегия»[553] касается проблем, связанных с выявлением сексуальных посягательств и потенциальных пробелов в преступлениях, связанных с распространением сфабрикованных сексуальных изображений.

Вопросы приемлемости также выявляют более широкую системную напряженность в случае записей, предположительно подделанных или сфабрикованных: если такие доказательства предположительно могли быть искажены или их достоверность становится проблемой, которая не может быть решена (напомним, что в настоящее время средства обнаружения глубоких фальшивок не существует), может быть нет другого выбора, кроме как исключить его на основании справедливости по отношению к обвиняемому[554]. Если использовать аналогию с судебно-медицинскими доказательствами expert[555], собранными на месте преступления, которые впоследствии могут быть подвергнуты сомнению или каким-либо образом испорчены[556], его часто исключают или уменьшают его вес. Если обвиняемый возьмет на себя бремя доказывания, вызывая у суда некоторый уровень сомнений в том, что аудиовизуальные материалы были сфабрикованы или сфабрикованы, можно

---

[553] «Стратегия борьбы с насилием в отношении женщин и девочек (VAWG) на 2017–2020 годы» (Лондон: CPS, 2017), https://www.cps.gov.uk/sites/default/files/documents/publications/VAWG-Strategy- 2017-2020.pdf. См. Также https://www.unwomen.org/en/what-we-do/ending-violence-against-women для более широкой стратегии самой Организации Объединенных Наций. Чесни и Ситрон подчеркивают аналогичную проблему, которую они называют «Дивидендом лжеца»: «Глубокие фальсификации облегчат лжецам возможность отрицать правду различными способами. Человек, обвиняемый в том, что что-то сказал или сделал, может вызвать сомнения в отношении обвинения, используя измененные видео- или аудиодоказательства, которые, по-видимому, противоречат утверждению. ... Глубокая подделка поможет избежать истины другим, не менее опасным способом. По иронии судьбы, лжецы, стремящиеся избежать ответственности за свои настоящие слова и действия, станут более авторитетными, поскольку общественность станет более осведомленной об угрозах, исходящих от глубоких фейков ». Роберт Чесни и Даниэль Ситрон, «Глубокие фейки: нависшая угроза конфиденциальности, демократии и национальной безопасности». там же, сноска 7, 1785.

[554] В английской системе издавна, либо в общем праве, либо в результате законодательства, существует право исключать доказательства, которые могут повлиять на справедливость судебного разбирательства. Однако, как показывает основной законодательный инструмент для этого усмотрения, раздел 78 (1) Закона 1984 года о полиции и доказательствах по уголовным делам, это обычно сосредоточено на доказательствах, представленных обвинением: «В любом судебном разбирательстве суд может отказать в разрешении доказательств по делу. на которое обвинение предлагает полагаться, если суду покажется, что с учетом всех обстоятельств, включая обстоятельства, при которых были получены доказательства, признание доказательств окажет такое неблагоприятное воздействие на справедливость судебное разбирательство, что суд не должен это признавать ». Согласно общему праву, судья имеет право по своему усмотрению в уголовном процессе «исключить доказательства, если это необходимо для обеспечения справедливого судебного разбирательства для обвиняемых» согласно лорду Гриффитсу в деле Скотт против Р. [1989] AC 1242, 1256, PC, со ссылкой на к многочисленным высказываниям на этот счет в Селви [1970] AC 304, HL и Санг [1980] AC 402, HL. В обоих случаях доказательства, представленные обвиняемым, не подпадают под один и тот же режим исключения.

[555] В вопросах науки или торговли, например, мнение эксперта или лица, близко знакомого с этой наукой или ремеслом, допустимо для предоставления суду информации, которая, вероятно, выходит за рамки опыта и знаний судьи или присяжных. . Только в том случае, если на основе доказанных фактов судья или присяжные могут сформировать свои собственные выводы без посторонней помощи, мнение эксперта будет ненужным: Turner (T.) [1975] QB 834; (1974) 60 Кр. Приложение. Р. 80, CA. См. В целом Mark Lucraft QC, Archbold: Criminal Pleading, Evidence & Practice 2020, (London: Sweet and Maxwell, 2020), 10-47.

[556] Обычно из-за неправильного обращения или ошибок в документации, которые оставляют веские основания утверждать, что образец был подделан или может не быть извлеченным. При рассмотрении действия доказательства, выходящего за рамки опыта или знаний суда, например, технических или экспертных доказательств, происхождение этих доказательств и цепочка хранения во время их анализа традиционно требовали полной прозрачности.

будет рассматривать ключевой источник доказательств, возможно, единственное подтверждающее доказательство в некоторых случаях, подобных тем, которые рассматриваются в делах о НОЖ как достаточно скомпрометированный, чтобы быть ненадежным и, следовательно, исключенным, что может создать проблемные прецеденты будущих дел.

Таким образом, суды могут обратиться к изучению технических систем, которые являются исходным происхождением самого материала, если они могут, и спросить, могла ли эта система реально каким-либо образом быть подделана. В системе видеонаблюдения возможность манипуляции с использованием генеративной технологии может быть менее вероятной, чем в более открытой системе. Если продолжить аналогию с судебно-медицинскими доказательствами, суды редко спрашивают, могли ли сами судебно-медицинские доказательства были подделаны. Если аналогичный подход будет применен к дип-фейкам, такой подход будет игнорировать технологически пониженные барьеры для входа, которые увеличивают разрушительный потенциал непризнанных и неосознанных возможностей: способность обычных людей создавать фальшивые кадры скоро будет намного больше, чем их возможности. для производства измененных образцов для судебной экспертизы из-за упомянутых нами технологических возможностей. Если запись смартфона может быть использована для обвинения или оправдания, может быть небезопасно полагаться на эти доказательства, если существует реальная перспектива того, что они могли быть сфальсифицированы[557].

Подделка и фальсификация возможны в контексте как аудио, так и видеозаписей, которые по-разному рассматриваются в английской системе, – любопытное несоответствие, которое само по себе выявляет некоторые важные проблемы[558]. Содержание аудиозаписей, даже если копии оригинала[559], если предъявлено и сыграно в суде[560], потому что аудиозапись считается

---

[557] Доказанная подлог может иметь значение, например, в силу факта ее подделки, а не из-за правдивости ее содержания, как ложь обвиняемого или лжесвидетельство другого свидетеля, при условии соответствующих предупреждений судьи первой инстанции.

[558] Точные причины раздельной эволюции вопросов допустимости аудио и визуальных доказательств выходят за рамки этой короткой статьи, но можно выдвинуть определенные гипотезы: например, тот факт, что аудиозапись
как технология предшествовала видеозаписи, может иметь значение, и аудио вполне могло, во время его поглощения в правовой среде, казаться достаточно похожими на заявления, содержащиеся в документах, чтобы считаться таковыми. Визуальный характер фотографии и видеозаписи достаточно различается, чтобы вызвать совершенно отдельный юридический анализ. Дальнейшие исследования по этому вопросу могут быть полезны для создания новой основы для регулирования допустимости аудио- и видеодоказательств в уголовных процессах в Англии и Уэльсе.

[559] Неважно, сколько удалений есть между копией и оригиналом, и что касается «аутентификации», в настоящее время считается, что суды, вероятно, потребуют такого же рода доказательств, которые были необходимы в случае копий в соответствии с общим правом, а именно надлежащее объяснение того, почему Оригиналы недоступны, и доказательство полной точности копий по отношению к оригиналу: Ормерод и Перри, Blackstone's Criminal Practice 2019, F8.53, со ссылкой на Робсона (июнь 1973 г., не сообщается) могут быть приняты в качестве доказательства их правдивости в соответствии с исключением из правила о слухах

[560] См., Например, Senat (1968) 52 Cr App R 282, который касался магнитофонных записей компрометирующих

«документом» для этих целей[561]. Было ли это подделано или сфабриковано – это совершенно отдельный вопрос. Без чего-то большего, на его лице есть опровержимая[562] презумпция правдивости[563]. И наоборот, очевидно[564], что видеодоказательства, например, из системы видеонаблюдения, не являются слухами. Фотографии и фильмы допустимы[565] по общему праву в качестве различных реальных доказательств[566]. Реальным доказательствам придается мало значения в отсутствие сопроводительных доказательств, идентифицирующих их и связывающих их с рассматриваемыми фактами. Любой, кто хочет представить запись в качестве доказательства, будь то аудио или видео, должен убедить суд в том, что доказательства подлинности и подлинности prima facie были доказаны путем вызова других доказательств, которые определяют и описывают происхождение и историю записи до момента ее предъявления в суде. Тем не менее, аутентичность относится исключительно к взаимосвязи между копиями и оригинальной записью, и редко делается акцент на возможности того, что оригинал сам по себе может быть

разговоров. Закон Англии и Уэльса всегда настаивал на том, что обычно необходимо, чтобы свидетельство истинности вопроса было дано лично свидетелем, который говорит на основании своих собственных наблюдений или знаний. В нем используется юридическое выражение «слух» для описания доказательств, которые не были даны, а скорее предоставлены из вторых рук, независимо от того, были ли они связаны с лицом, с которым разговаривал отсутствующий свидетель, содержащимся в письменном заявлении отсутствующего свидетеля, приведенном в форма документа или записи, созданной им, или иным образом ». (Хорнкасл [2010] 2 AC 373, лорд Томас CJ). Такие свидетельства из вторых рук не воспринимаются как низшие по сравнению с первичными доказательствами, которые могут быть проверены в ходе судебного процесса, будь то перекрестный допрос или другие средства судебной экспертизы.

[561] Закон об уголовном правосудии 2003 г., с. 133 и с. 134 (1).

[562] В случае компьютерных распечаток, которые могут служить подтверждением аналогичных аргументов, прежде чем судья сможет решить, допустимы ли они в качестве реальных доказательств или слухов в соответствии с законом, необходимо вызвать соответствующие авторитетные доказательства для описания функции и работа компьютера (Cochrane [1993] Crim LR 48).

[563] См., Например, публичное онлайн-заявление онлайн-правового руководства CPS в отношении экспонатов, где с точки зрения доказательства «подлинности» видеозаписи обвинение должно иметь возможность показать, что «видеопленка, представленная в качестве доказательства, является оригинальная видеозапись или подлинная копия оригинала »и показать, что она« не была подделана ». Для этого должны быть доступны заявления, которые представляют видеодоказательства в качестве вещественных доказательств и обеспечивают их целостность и безопасность. Никакого упоминания о его правдивости или чего-либо подобного не делается. «Правовое руководство CPS: экспонаты», последняя редакция: 9 апреля 2018 г. (https://www.cps.gov.uk/legal-guidance/exhibits).

[564] Из определения «заявления» в разделе 115 (1) Закона 2003 г. как изложение факта или мнения, сделанного человеком (как в случае с аудиозаписью).

[565] Фотография или фильм, релевантность которых может быть установлена на основании показаний лица, лично осведомленного об обстоятельствах, в которых они были сделаны или сделаны, могут быть допустимы. Присяжным разрешается просматривать фотографии, сделанные камерой наблюдения во время вооруженного ограбления (Додсон [1984] 1 WLR 971), или видеозаписи инцидента (Фоуден [1982] Crim LR 588; Grimer [1982] Crim LR 674).

[566] Реальным доказательством обычно является какой-либо материальный объект, существование, состояние или ценность которого является предметом спора или имеет отношение к вопросу, представленный в суде для проверки трибуналом по фактам. В Статуе Свободы [1968] 2 All ER 195, где фильм, по сути, содержал заявление о путях, пройденных двумя кораблями, сэр Джоселин Саймон П. отвергает заявление, которое записала кинематографическая пленка с радарным эхом. от береговой радиолокационной станции, было недопустимо, потому что оно было произведено механически без вмешательства человека, говорится (на стр. 740): «Если записи на магнитную ленту допустимы, кажется, что фотография приема радиолокатора также допустима - или, действительно, любой другой тип фотографии. Было бы абсурдным различие, что фотография была бы допустима, если бы фотоаппарат управлялся вручную фотографом, но не, если бы он управлялся с помощью механизма отключения или часов ».

сфабрикованным[567]. Проблема для судов сейчас, как мы уже сказали, заключается в правдивости: что оригинал может сам по себе является вымыслом и больше не представляет собой надежного и точного описания того, что он призван представлять. Как мы покажем, это представляет собой двустороннюю дилемму.

Позиционирование содержания аудиовизуальной записи в рамках различных режимов допустимости является функцией чего-то хорошо известного: по мере развития технологий закон развивается вслед за ним, обычно недостаточно быстро, чтобы с ним справиться, и не достаточно всесторонне, чтобы охватить что-то большее, чем суть поставленной проблемы. Эта расходящаяся эволюция в отношении аудио и видеозаписей скоро станет совершенно несостоятельной, особенно там, где такие типы доказательств чаще объединяются, поскольку они неизбежно будут в эпоху повсеместного распространения смартфонов.

Комбинаторные возможности: подделки в контексте повсеместности

Попытки проанализировать влияние искусственного интеллекта исключительно с точки зрения придуманных возможностей упускают из виду разнообразные проблемы, возникающие в результате того, как субъекты осознают и используют возможности, которые предоставляют технологии. Изобретенные аффордансы – это самая легкая проблема, с которой можно столкнуться, только когда игнорируются их комбинации с другими технологиями. Кроме того, непризнанные и неиспользованные аффордансы подвергаются комбинаторному взрыву, когда они пересекаются с дополнительными возможностями, предоставляемыми другими технологиями. Истинное влияние фейков, мы предполагаем, что их можно найти в их сочетании с почти повсеместной возможностью цифровой аудиовизуальной записи за счет широкого внедрения смартфонов, простоты совместного использования таких аудиовизуальных записей, обеспечиваемого постоянным взаимодействием и облачными системами, а также нормативным социальным и экономическим контекстом, в котором такое совместное использование

[567] Некоторую озабоченность в контексте наших аргументов вызывает прецедент, разрешающий доказывать видеодоказательства условно-досрочными показаниями свидетелей, которые видели фотографию или фильм. В деле Тейлор против главного констебля Чешира [1986] 1 All ER 225, видеозапись с видеокассеты, сделанная камерой наблюдения и показывающая человека в магазине, который берет предмет и кладет его в свою куртку, была воспроизведена полицейским, которые опознали человек как Тейлор. Запись после того, как ее вернули в магазин, случайно стерли. Доказательства со стороны офицеров того, что они видели на видео, были сочтены признанными должным образом на том основании, что то, что они видели на видео, в принципе не отличалось от свидетельств очевидца, который действительно был свидетелем инцидента, несмотря на факт, что свидетели могут быть допрошены на предмет истинности их показаний.

ожидаемо. Это распространение цифрового аудиовизуального материала в сочетании с пониженными барьерами для глубоко подделки и манипуляции создает более общую и повсеместную эпистемическую неопределенность относительно правдивости любого аудиовизуального материала.

Поэтому мы предполагаем, что, хотя изобретенные аффордансы, предоставляемые дип-фейками, могут сами по себе создать первоначальные проблемы для взвешивания улик, их влияние оставалось бы относительно ограниченным без дополнительных изобретенных аффордансов, представленных возможностями смартфонов и облачных вычислений. Несмотря на это, гораздо большее беспокойство вызывают возможности распознавания и эксплуатации: в нашем примере и, вероятно, есть много других, это связано с осознанием того, что глубоко фальшивые манипуляции и фабрикация могут быть связаны с распространением видео и аудио со смартфонов, и использование этой реализации[568]. Другими словами, эпистемологические проблемы, возникающие из-за возможности того, что все видео и аудио могут быть изменены или сфабрикованы, просто не существовали бы без более широкого контекста, в котором цифровое аудио и видео являются повсеместными, а также уязвимы для глубоких подделок.

Контрастное диффузное использование смартфона с закрытыми системами, такими как видеонаблюдение, где обычно можно определить первоначальное происхождение рассматриваемого материала и, вероятно, исключить вероятность помех. Однако в эпоху капитализма слежки[569], когда социальные сети поощряют запись и обмен повседневной жизнью и опытом, когда Интернет вещей становится повсеместной реальностью, и где смартфоны в руках миллиардов граждан обладают не только высококачественным видео возможности, но емкость для хранения таких видео, существует вполне реальная перспектива представления видео и аудио доказательств, которые поступают не из закрытых систем. Такие материалы вполне могут показаться имеющими отношение к рассматриваемым фактам – действительно, в случае серьезного сексуального посягательства или изнасилования, которые в настоящее время снова привлекают внимание средств массовой информации

---

[568] Подробный анализ см. В Роберте Чесни и Даниэль Ситрон, «Глубокие фейки: надвигающаяся угроза конфиденциальности, демократии и национальной безопасности». там же, снос 7. Также Катарина Кертысова. «Искусственный интеллект и дезинформация: как ИИ меняет способы производства, распространения и противодействия дезинформации». Безопасность и права человека 29 (2018) 55-81, 67 (обсуждение «растущей простоты создания и распространения поддельного видео- и аудиоконтента на компьютерах и мобильных устройствах», создающих широкие возможности для «запугивания, шантажа и саботажа за пределами политики. и международные дела». Европол также недавно отметил возможность преступного использования технологии глубокого подделки: Европол, «Мечтают ли преступники об электрических овцах?» Агентство Европейского Союза по сотрудничеству в правоохранительной сфере 2019, 10.

[569] Литература в этой области обширна и подходит к комплексу вопросов с самых разных точек зрения, но для всестороннего анализа см. Шошана Зубофф, Эпоха слежки за капитализмом: борьба за будущее человечества на новых рубежах власти. Нью-Йорк: Связи с общественностью, 2019 г. и Джули Э. Коэн, Между истиной и властью: правовые конструкции информационного капитализма, Оксфорд: OUP, 2019.

из-за обвинений в неприемлемом подходе к судебному преследованию со стороны Королевской прокуратуры[570] и, как следствие, низким уровнем обвинительных приговоров[571], доказательства со смартфонов могут предоставить убедительные косвенные доказательства поведения, приведшего к предполагаемому нападению, будь то обвинительное или оправдательное. Наш анализ демонстрирует громоздкий, разрозненный подход к аудио и визуальным свидетельствам в английской системе, пытаясь приспособить их или исключить из уже существующих доктрин, таких как слухи или реальные свидетельства, но аудио- и видео свидетельства в контексте повсеместности, как мы утверждаем, больше не подходит ни одной существующей категории и требует совершенно нового подхода: отдельной категории со своим собственным режимом доказывания.

Арена преступлений против насилия в отношении женщин также выявляет другие континуумы между аффордансами. Мы утверждаем, что у дип-фейков есть потенциал как для создания новых правонарушений, которых в настоящее время не существует, так и для новых способов совершения существующих правонарушений. Мы проиллюстрируем противоречие между неосознанными и неиспользованными аффордансами и медлительность закона, чтобы предвидеть их, с помощью краткого анализа раздела 33 закона об уголовном правосудии и судах 2015 года, который недавно объявил преступлением разглашение личных сексуальных фотографий или фильмов без согласия человека, который появляется в них, и с намерением причинить этому индивидууму страдания[572].

Изготовленные с порнографическими изображениями будут отображаться не будут охвачены offence[573], который составлен таким образом,

---

[570] Келинн Барр, Александра Топпинг и Оуэн Боукотт, «Преследования изнасилований в Англии и Уэльсе на самом низком уровне за десятилетие», The Guardian, 12 сентября 2019 г., https://www.theguardian.com/law/2019/sep/ 12/судебное преследование в англии и уэльсе на самом низком уровне за десятилетие.

[571] Келейн Барр и Оуэн Боукотт, «Падение числа обвинительных приговоров за изнасилование« из-за критической системы правосудия»», The Guardian, 19 декабря 2019 г., https://www.theguardian.com/law/2019/dec/17/fall -в судимости-из-за-система правосудия-на грани разрыва.

[572] Один из связанных с этим серьезных пробелов в этом правонарушении, который демонстрирует более широкое непонимание взаимосвязи между социальными сетями и репутацией, относится к его mens rea: человек будет виновен в правонарушении только в том случае, если причина раскрытия фотографии или одна из причин - причинить страдания человеку, изображенному на фотографии или пленке. Любой, кто отправляет сообщение только потому, что считает его забавным, не совершает преступления. Это кажется поразительным пробелом, учитывая вызванный эмоциональный стресс и потенциально необратимый репутационный ущерб, который, вероятно, будет одним и тем же независимо от намерений отправителя.

[573] Правовое руководство Королевской прокуратуры по данному правонарушению, составленное до того, как глубокие подделки стали настолько распространенными в общественном сознании, демонстрирует, как быстро технологические достижения могут сделать законодательство устаревшим. Учитывая, что это руководство частично помогает определить, какие правонарушения преследуются по закону, мы полагаем, что оно полезно для оценки эффективности правонарушения. «КПС правовой Guidance: Месть Порнография - Руководство по преследованию за преступления, раскрытие частных сексуальные фотографий и фильмов», пересмотренные 24 января 2017, чтобы добавить раздел Секстинг https://www.cps.gov.uk/legal-guidance/revenge- порнография-принципы, преследование, преступления-раскрывающую-частного сексуальна.

что это относится только к материалу, который берет свое начало от оригинальной фотографии или фильма recording.'[574] Это, Королевская прокурорская служба утверждает в своей правовой ориентации для прокуроров, это потому, что «вред, который должен быть устранен в результате правонарушения, – это неправомерное использование фотографий или фильмов интимного характера». Является ли вред поддельного видео, которое выглядит реальным, меньше, чем вред подлинного изображения или распространенного видео? Мы предполагаем, что ответ должен быть отрицательным[575]. Таким образом, технология глубокого подделки создает новые средства совершения старых правонарушений, даже относительно недавно составленных правонарушений, которые не вписываются в существующие системы обнаружения, виновности или доказывания. Раздел 33 представляет собой пример закона и его институтов, которые едва успевают за технологическими изменениями.

Обсуждение вопроса о допустимости записей со смартфона обнаруживает еще одну напряженность. В английской системе для достижения равенства сторон в состязательном процессе правила исключения, как правило, применяются в большей степени к доказательствам, представленным обвинением, чем обвиняемым. Очевидно, что у государства традиционно гораздо больше шансов располагать соответствующими и доступными техническими доказательствами, такими как аудио- или видеозаписи, чем у отдельного обвиняемого. В эпоху смартфонов этого больше не будет. Представьте себе обвинение в изнасиловании во время вечеринки. Доказательства соответствующего предшествующего поведения фиксируются потерпевшим или другими участниками партии, которые являются свидетелями обвинения, а также обвиняемым или другими участниками партии, у которых есть доказательства, относящиеся к подсудимому. Различные вопросы о допустимости будут применяться к идентичным типам доказательств,

---

[574] «КПС правовая Guidance: Месть Порнография», там же . Преступление не включает ситуации, когда изменение или комбинация фильма или фотографии только затем делает их сексуальными, или если предполагаемая жертва изображается только в сексуальном плане в результате изменения или комбинации. Так, например, человек, который просто переносит голову бывшего партнера на сексуальную фотографию другого человека, что является обычным способом использования технологии глубокой подделки, не совершит преступления. Более того, изображения, которые «полностью сгенерированы компьютером, но выглядят как фотография или фильм, не подпадают под состав преступления».

[575] CPS, похоже, поддерживает эту позицию в дальнейших рекомендациях, касающихся гораздо более старого законодательства, датированного 1988 годом: сообщения, отправленные через социальные сети, могут включать

в себя совершение ряда существующих преступлений против личности, общественного правосудия, нарушения сексуального права или общественного порядка. как совершение коммуникативных преступлений, противоречащих разделу 1 Закона о вредоносных коммуникациях 1988 года и / или разделу 127 Закона о коммуникациях 2003 года: «Правовое руководство CPS: социальные сети - Руководство по судебному преследованию дел, связанных с сообщениями, отправленными через социальные сети», пересмотрено: 21 Август 2018 г. https://www.cps.gov.uk/legal-guidance/social-media-guidelines-procowing-cases-involving-communications-sent-social-media.

полученных с помощью идентичных технических средств. В какой степени ответчик должен будет доказать, если вообще доказать, что доказательства, представленные в его защиту, не являются фальшивкой, учитывая, что это именно то, что может потребовать сделать Корона?

Эта напряженность усиливается при рассмотрении ресурсов и богатства таких организаций, как корпорации, обвиняемые в мошенничестве с «белыми воротничками», террористические группы или организованные преступные сети. Если способность отдельного лица сохранить фальсифицированную или сфабрикованную аудио- или видеозапись кажется изначально фантастической, то в случае с такими богатыми и связанными организациями, для которых возникает такое же напряжение допустимости, это гораздо хуже. Например, одним из способов доказательства наличия террористических объединений является подтверждение интервью, данных предполагаемыми террористами средствам массовой информации в таких регионах, как Сирия. Эти допросы неизбежно редактируются, что само по себе приводит к одной категории вопроса о допустимости, но возникают более серьезные проблемы, если подозреваемый заявляет, что его вообще не допросили, а видео является полностью сфабрикованным. Учитывая силу дезинформации и кибервойны в таких конфликтах низкой интенсивности, это утверждение может иметь какое-то основание, однако получение оригинала или доказательств от составителя может оказаться невозможным. И наоборот, если бы аудиовизуальные доказательства алиби были представлены, чтобы продемонстрировать, что ответчик не мог быть допрошен, он вполне мог бы подпадать под другой стандарт.

Могут быть предусмотрены ситуации, когда глубокие подделки могут также привести к криминализации тех, кто до сих пор, когда правонарушения требовали большего физического, финансового или эмоционального участия и риска, могли не совершать эти правонарушения или чье поведение могло считаться относительно незначительным, когда ранее более автономный. Глубокие фейки в контексте повсеместности представляют собой смену парадигмы в том, с какой легкостью пользователи смартфонов могут поддаться соблазну, например, в отношении мошенничества, шантажа или преследований. В ситуациях сильного эмоционального возбуждения или возбуждения, когда рациональное мышление нарушено, технологии теперь предлагают немедленные возможности.

Такие правонарушения можно рассматривать как совершенно новые, подлинные, а затем и непредвиденные последствия новых технологий для ничего не подозревающего общества или как разновидность старых преступлений, которые превратились в нечто иное и непредвиденное. Для всех практических целей это различие может не иметь значения и, возможно, даже

демонстрирует тот факт, что аффордансы в этой структуре не являются дискретными и фиксированными, а скорее континуумами, по которым аффордансы движутся, развиваются и сочетаются с течением времени и с достижениями в науке и технологиях. Ясно, что последствия таких достижений не всегда можно предсказать: их следует рассматривать как «неощутимые аффордансы», а исторический анализ в этой области обнаруживает новое поведение, которое регулировалось путем криминализации.

Заключительные мысли

Мы предположили, что существует двухэтапная проблема, которую создают глубокие подделки при содействии GAN для систем уголовного правосудия. На первом этапе, когда они рассматриваются изолированно, глубокие подделки создают ограниченную проблему, касающуюся их доказательной правдивости, которая, вероятно, может быть разрешена надежной судебной системой. Однако на втором этапе комбинаторный характер аффордансов, представленных дип-фейками, сочетается с повсеместным контекстом аудиовизуальной записи и тиражирования, чтобы подорвать неявные, но фундаментальные эпистемологические предположения. Если воспринимать их серьезно, такие эрозии угрожают самой возможности полагаться на широкие категории доказательств в уголовном процессе. Такой анализ становится возможным не благодаря изучению внутренней природы и характеристик искусственного интеллекта и не путем анализа его конкретных приложений, а, скорее, путем помещения эффектов в концептуальные рамки аффордансов. Тем не менее, даже такого исследования недостаточно, чтобы по-настоящему понять будущие проблемы, и только посредством более детального анализа с использованием комбинаторного подхода мы даже начнем заниматься надвигающимися фундаментальными сдвигами в социотехническом ландшафте.

Это упражнение намекает на косвенный характер проблем, создаваемых ИИ для уголовного правосудия, которые нельзя выделить заранее, и является убедительным подтверждением дилеммы Коллингриджа[576]. Наше предложение о попытках сформулировать ответные меры уголовного правосудия на вызовы ИИ выходит за рамки предлагаемой здесь концептуальной структуры аффордансов (что является лишь одним из возможных подходов) и предлагает нам посмотреть, как внедрение технологии сочетается с существующим

[576] Дэвид Коллингридж, Социальный контроль технологий (Фрэнсис Пинтер, 1980). Его можно кратко резюмировать следующим образом: «Когда перемены просты, необходимость в них предвидеть невозможно; когда изменения очевидны, они становятся дорогостоящими, трудными и требуют много времени», 11.

социотехническим ландшафтом, так и с признанными и потенциальными применениями других новых и появляющихся технологий. Вполне вероятно, что, хотя ИИ в отдельности будет создавать серьезные проблемы, более фундаментальные вопросы будут лежать в лагранжевых точках между новыми технологиями.

Ссылки

IEEE Conference on Computer Vision and Pattern Recognition Workshops (2019): 38–45.

Айдер, Генри, Джорджио Патрини, Франческо Кавалли и Лоуренс Каллен. «Состояние глубоких подделок: ландшафт, угрозы и влияние». Deeptrace Labs, сентябрь 2019 г.

Ариэли, Дэн. Предсказуемо иррационально: скрытые силы, определяющие наши решения. Лондон: Харпер, 2009.

Балкин, Джек М. «Путь закона робототехники». California Law Review Circuit 6 (2015): 45–60.

Барнс, Кертис и Барраклаф, Том. «Perception Inception: подготовка к дипфейкам и синтетическим медиа завтрашнего дня». Фонд права Новой Зеландии, 21 мая 2019 г., https://www.brainbox.institute/report.

Барр, Кэленн, Александра Топпинг и Оуэн Боукотт. «Преследования изнасилований в Англии и Уэльсе на самом низком уровне за десятилетие». The Guardian, 12 сентября 2019 г., https://www.theguardian.com/law/2019/sep/12/proservations-in-england-and-wales-at-lowest-level-in-a-decade.

Барр, Келейн и Оуэн Баукотт. «Снижение числа осужденных за изнасилование «из-за критической системы правосудия». The Guardian, 19 декабря 2019 г.,

https://www.theguardian.com/law/2019/dec/17/fall-in-convictions-due-to-justice-system-at-breaking-point.

Кало, Райан. «Политика в области искусственного интеллекта: учебник и дорожная карта». UCDL Ред. 51 (2017): 399-435.

Чандер, Анупам. «Расистский алгоритм?» Мичиган Л. Rev.115 (2017): 1023

Чесни, Роберт и Даниэль Китс Ситрон. «Глубокие подделки: надвигающийся вызов конфиденциальности, демократии и национальной безопасности». California Law Review 107, no. 6 (1 декабря 2019 г.): 1753

Чесни, Роберт и Даниэль Китс Ситрон. «Распад правды в стиле 21-го века: глубокие подделки и вызов конфиденциальности, свободе выражения мнений и национальной безопасности». Обзор закона Мэриленда 78, нет. 4 (2019): 882-891.

Чесни, Роберт, Даниэль Ситрон и Кинта Юречич. «Это видео Пелоси: что делать с « дешевыми фейками »в 2020 году». Lawfare (29 мая 2019 г.),

https://www.lawfareblog.com/about-pelosi-video-what-do-about-cheapfakes-2020.

Коэн, Джули Э., Между правдой и властью: правовые конструкции информационного капитализма. Оксфорд: ОУП, 2019.

Королевская прокурорская служба. «КПС правовых принципы: Месть Порнография - Руководство по преследованию за преступления, раскрытие частных сексуальные фотографий и фильмов», редакция: 24 января 2017 года, чтобы добавить раздел на секстинге.

https://www.cps.gov.uk/legal-guidance/revenge-pornography-guidelines-procowing-offence-disclosing-private-sexual.

Королевская прокурорская служба. «Стратегия борьбы с насилием в отношении женщин и девочек (НОЖГ) на 2017–2020 годы». (Лондон: CPS, 2017),

https://www.cps.gov.uk/sites/default/files/documents/publications/VAWG-Strategy-2017-2020.pdf.

Королевская прокурорская служба. «Правовое руководство CPS: Экспонаты». исправлено: 9 апреля 2018 г. (https://www.cps.gov.uk/legal-guidance/exhibits).

Королевская прокурорская служба. «Правовое руководство CPS: социальные сети - Руководство по судебному преследованию дел, связанных с сообщениями, отправленными через социальные сети». доработана: 21 августа 2018 г.

https://www.cps.gov.uk/legal-guidance/social-media-guidelines-procowing-cases-involving-communications-sent-social-media.

Коллингридж, Дэвид. Социальный контроль технологий. Фрэнсис Пинтер, 1980

Дикс, Эшли. «Судебное требование объяснимого искусственного интеллекта», Columbia Law Review, 119, вып. 7 (2019): 1829-50.

Европол, «Мечтают ли преступники об электрических овцах?» Агентство Европейского Союза по сотрудничеству в правоохранительной сфере, 2019.

«Fakta: Flest har fået bøder i Umbrella-sagen». Jyllandsposten, 25 января 2020 г.

https://jyllands-posten.dk/indland/politiretsvaesen/ECE11899455/fakta-flest-har-faaet-boeder-i-umbrellasagen/.

Фарид, Хани. «Судебная экспертиза изображений». Ежегодный обзор Vision Science 5, номер 1 (2019): 549-573.

Фрэнкс, Мэри Энн и Ари Эзра Уолдман. «Секс, ложь и видеозаписи: фейки и заблуждения о свободе слова». Обзор закона Мэриленда 78, нет. 4 (2019): 892-898.

Гарфинкель, Бен и Аллан Дефо. «Как изменяется баланс между атакой и защитой?» Журнал стратегических исследований. 42, vol.26 (2019): 736-763.

Главяну, Влад П .. «Что можно сделать с яйцом? Творчество, материальные объекты и теория денег ". Журнал творческого поведения 46, № 3 (2012): 192–208.

Гибсон, Джеймс Дж. Экологический подход к визуальному восприятию. Хиллсдейл, Нью-Джерси: Эрлбаум, 1986.

Холл, Холли Кэтлин. «Фальшивые видео: когда видишь - не веришь». Журнал права и технологий Католического университета 27, вып. 1 (осень 2018 г.): 51-76.

Гамильтон, Ребекка Дж. «Новые технологии в международных уголовных расследованиях». Материалы ежегодного собрания ASIL 112 (2018): 131–33. DOI: 10.1017/amp. 2019.18.

Гамильтон. «Доказательства, созданные пользователями». Колумбийский журнал транснационального права 57, № 1 (2018) Американский университет, Исследовательский доклад WCL № 2018-11.

Канеман, Даниэль. Мыслить быстро и медленно. Лондон: Penguin Allen Lane, 2012.

Клитгаард, Мадс. «Я в Дании делает ставку на сексуальные тапочки с удобными носками». Берлингске, 29 августа 2019 г. https://www.berlingske.dk/samfund/i-en-af-danmarks-stoerste-sager-om-deling-af-seksuelle-optagelser-slipper

Лю, Хин-Ян, Маттис Маас, Джон Данахер, Луиза Скарчелла, Микаэла Лексер и Леонард Ван Ромпей. «Искусственный интеллект и нарушение законодательства: новая модель анализа». Право, инновации и технологии 12, № 2 (2020).

Lucraft QC, Марк. Archbold: представительство по уголовным делам, доказательства и практика, 2020. Лондон: Sweet and Maxwell, 2020.

Кертысова, Катарина. «Искусственный интеллект и дезинформация: как ИИ меняет способы производства, распространения и противодействия дезинформации». Безопасность и права человека 29 (2018) 55-81.

Марас, Мари-Элен и Алекс Александру. «Определение подлинности видеодоказательств в эпоху искусственного интеллекта и после появления видео Deepfake». Международный журнал доказательств и доказательств 2019, Vol. 23 (3) 255–262.

Марку, Кристофер. «Почему использование ИИ для вынесения приговора преступникам - опасная идея». Разговор, 16 мая 2017 года.

https://theconversation.com/why-using-ai-to-sentence-criminals-is-a-dangerous-idea-77734.

Михельфельдер, Дайан. «Постфеноменология с оглядкой в будущее». В постфеноменологических исследованиях: очерки отношений между людьми и технологиями, под редакцией Роберта Розенбергера и Питера-Пола Вербека, 237–46. Лэнхэм: Lexington Books, 2015.

Норман, Дональд А. Дизайн повседневных вещей. Кембридж, Массачусетс: MIT Press, 2016.

О'Нил, Кэти. Оружие разрушения математики: как большие данные увеличивают неравенство и угрожают демократии. Лондон: Penguin Allen Lane, 2016.

Ормерод, QC, Дэвид, и Дэвид Перри, QC. Криминальная практика Blackstone 2019. Оксфорд: OUP, 2019.

Питерс, Джей. «Alphabet's Jigsaw представляет инструмент, который помогает журналистам обнаруживать глубокие подделки и фальшивые изображения». The Verge, 4 февраля 2020 года.

https://www.theverge.com/2020/2/4/21122778/alphabet-jigsaw-assembler-tool-news-journalists-deep-fakes-images)

Рademахер, Тимо. «Искусственный интеллект и правоохранительные органы». В разделе «Регулирование искусственного интеллекта», под

редакцией Томаса Вишмайера и Тимо Рademахера, 226–255. Чам, Швейцария: Springer, 2020.

Сассер, Даниэль. «Невидимое влияние: искусственный интеллект и этика архитектурного выбора» на конференции AAAI / ACM по ИИ, этике и обществу (AIES '19). Нью-Йорк, Нью-Йорк: ACM, 2019. https://doi.org/10.1145/3306618.3314286.

Сассер, Даниэль. «Прозрачные СМИ и развитие цифровых привычек». В Постфеноменологии и СМИ: Очерки отношений между людьми, технологиями и миром, под редакцией Йони Ван Ден Эде и др., 27-44. Лэнхэм: Lexington Books, 2017.

Талер, Ричард Х. и Касс Р. Санстейн. Подталкивание: принятие решений о здоровье, богатстве и счастье. Лондон: Penguin Allen Lane, 2009.

Винсент, Джеймс. «Алгоритмов обнаружения глубоких подделок никогда не будет достаточно». The Verge, 27 июня 2019 года.

https://www.theverge.com/2019/6/27/18715235/deep-fakes-detection-ai-algorithms-accuracy-will-they-ever-work.

Волкерт, Роберт и Генри Аджер, «Анализ коммодитизации глубинных подделок». Журнал законодательства и государственной политики Нью-Йоркского университета. 27 февраля 2020 г. https://nyujlpp.org/quorum/volkert-ajder-analyzing-the-commoditization-of-deep-fakes/ (получено 28 февраля 2020 г.).

Зубофф, Шошана. Эпоха надзорного капитализма: борьба за человеческое будущее на новых рубежах власти. Нью-Йорк: Связи с общественностью, 2019.

Искусственный интеллект и правоохранительная информация: использование аналитики, управляемой ии, для борьбы с секс-торговлей

Клотильда Себаг [577]

В этом документе рассматривается использование аналитики на основе искусственного интеллекта правоохранительными органами для борьбы с торговлей людьми в целях сексуальной эксплуатации и оценивается влияние этого на правоохранительные органы. Полицейские органы по всему миру все

[577] Клотильда Себаг - научный сотрудник Института безопасности и глобальных отношений Лейденского университета. Работая в группе исследований разведки и безопасности, она интересуется взаимосвязью между международной безопасностью, разведкой и организованной преступностью.
Искусственный интеллект и робототехника для правоохранительных органов (Интерпол и ЮНИКРИ, 2019 г.), т.
https://issuu.com/unicri/docs/artificial_intelligence_robotics_la/1?ff.

чаще используют аналитическое программное обеспечение на основе искусственного интеллекта, чтобы помочь им в борьбе с торговлей людьми в целях сексуальной эксплуатации, поскольку эта технология теперь позволяет собирать, обрабатывать и анализировать огромные объемы онлайн-данных, оставленных торговцами людьми. Возможность сделать это привела к распространению подхода к полицейской деятельности, известного как полицейское управление на основе данных – с помощью действенной информации в реальном времени, предоставляемой аналитическим программным обеспечением на основе искусственного интеллекта, правоохранительные органы могут разрабатывать гораздо более активные и подробные ответные меры. Однако эта зависимость от данных также вызывает беспокойство, поскольку качество аналитики, производимой с помощью аналитики на основе ИИ, настолько хорошо, насколько хороши данные, которые он обрабатывает. Пробелы в данных и вводящие в заблуждение данные могут ослабить реакцию полиции. Более того, также высок риск разработки непонятных и необъяснимых систем ИИ. Правоохранительным органам рекомендуется создать основу, которая будет определять внедрение технологий искусственного интеллекта в этой области. В целом, использование аналитики на основе искусственного интеллекта для борьбы с торговлей людьми в целях сексуальной эксплуатации показывает, как сегодня предотвращение преступности находится на стыке технологий и данных.

Ключевые слова: искусственный интеллект, аналитика на основе искусственного интеллекта, торговля людьми с целью сексуальной эксплуатации, данные, правоохранительные органы, анализ, проактивная политика, основанная на данных, черный ящик, пробелы в данных, структура искусственного интеллекта.

Вступление

В рамках все более широкого использования искусственного интеллекта (ИИ) в правоохранительных органах сообщество по борьбе с торговлей людьми сосредоточило внимание на том, как технологии могут помочь в борьбе с торговлей людьми в целях сексуальной эксплуатации. В центре этого – «усилия, основанные на данных»[578] с государственными и частными инициативами, направленными на реструктуризацию того, как проводятся расследования торговли людьми с целью сексуальной эксплуатации, за счет использования возможностей искусственного интеллекта, данных и

[578] Мария Майорга и др., «Противодействие торговле людьми с использованием методов ISE / OR», в Emerging Frontiers in Industrial and Systems Engineering: Success through Collaboration, под ред. Гарриет Б. Нембхард, Элизабет А. Кадни и Кэтрин М. Коперих (CRC Press, 2019), 245, PDF.

расширенной аналитики[579].

Была выбрана для использования термина «аналитика на основе ИИ» для описания применения технологий ИИ к расширенным аналитическим возможностям. Первоначально он был разработан для предприятий, но в настоящее время используется правоохранительными органами, прокуратурой и неправительственными организациями (НПО) по всему миру для борьбы с торговлей людьми в целях сексуальной эксплуатации и расследования дел. Действительно, аналитика на основе искусственного интеллекта помогает спасти сотни жертв и предоставить необходимые сведения для борьбы с торговцами людьми. Некоторые из самых популярных сегодня программ включают Memex, Traffic Jam, XIX и Spotlight.

Аналитика на основе искусственного интеллекта оказала глубокое влияние на возможности правоохранительных органов по предотвращению преступности и является одной из наиболее широко применяемых технологий искусственного интеллекта полицейскими ведомствами по всему миру. Таким образом, его практическое применение в расследованиях торговли людьми в целях сексуальной эксплуатации заслуживает тщательного изучения, чтобы лучше понять его влияние на подходы, взгляды и возможности правоохранительных органов. Изучение этого конкретного приложения также помогает пролить свет на более широкие преимущества и проблемы интеграции большего количества технологий искусственного интеллекта в полиции. Эта статья начинается с контекстуализации того, что подразумевается под торговлей людьми с целью сексуальной эксплуатации; затем анализируется аналитика на основе ИИ – как работает эта технология и как она применяется на практике для пресечения торговли людьми в целях сексуальной эксплуатации. Наконец, он оценивает основные воздействия, которые он оказывает на правоохранительные органы.

Было обнаружено, что аналитика, основанная на искусственном интеллекте, чрезвычайно полезна для правоохранительных органов, чтобы получить более полное представление о моделях и тенденциях торговли людьми в целях сексуальной эксплуатации, а также предоставить бесценные сведения для расследований и операций. Более того, использование аналитики на основе искусственного интеллекта отражает продолжающийся сдвиг в правоохранительных органах в сторону большей зависимости от больших данных, что приводит к все более и более основанному на данных подходу к контролю над политикой[580]. С экспоненциальным ростом объема данных закон

---

[579] Кэти Какенмайстер, «ИИ и борьба с торговлей людьми», Университет Лихай, последнее изменение 30 октября 2019 г., по состоянию на 3 марта 2020 г., https://engineering.lehigh.edu/news/article/ai-and-fight- против торговли людьми.

[580] Эндрю Гатри Фергюсон, Рост полицейской работы с большими данными: наблюдение, расы и будущее правоохранительных органов (Нью-Йорк: New York University Press, 2017), 16.

правоприменения по-прежнему будет требовать мощных аналитических возможностей для его обработки и анализа. Таким образом, как показывают усилия по борьбе с торговлей людьми, борьба с преступностью все чаще осуществляется на стыке технологий и данных.

Контекстуализация сексуальной торговли

Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН) делит торговлю людьми на три категории: торговля людьми в целях сексуальной эксплуатации; торговля людьми с целью принудительного труда; и торговля в других целях. Хотя модели торговли людьми и наиболее распространенные формы эксплуатации различаются по всему миру, наиболее обнаруживаемой формой является торговля людьми с целью сексуальной эксплуатации, причем 59 процентов выявленных жертв в 2016 году стали жертвами торговли людьми по этой причине. Вторая по распространенности форма торговли людьми – принудительный труд, который составляет 33 процента выявленных жертв. Тем не менее, в наших знаниях о характере торговли людьми остаются значительные пробелы, и в значительной степени преобладает безнаказанность[581].

Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, также известный как Палермский протокол, был принят Организацией Объединенных Наций в 2000 году с целью определения международного подхода к борьбе с торговлей людьми. Он устанавливает международно признанное определение «торговли людьми» в его статье 3:

Вербовка, транспортировка, передача, укрывательство или прием людей посредством угрозы силой или ее применения или других форм принуждения, похищения, мошенничества, обмана, злоупотребления властью или уязвимым положением или предоставление или получение выплат или пособий для достижения согласия лица, контролирующего другое лицо, с целью эксплуатации. Эксплуатация включает, как минимум, эксплуатацию проституции других лиц или другие формы сексуальной эксплуатации, принудительный труд или услуги, рабство или обычаи, сходные с рабством, подневольным состоянием или извлечением органов[582].

---

[581] 7 УНП ООН, Глобальный отчет о торговле людьми 2018, 13, 14, 29, 31 декабря 2018 г., по состоянию на 11 февраля 2020 г., https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf.

[582] Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной

Агентство Европейского Союза по обучению правоохранительных органов (CEPOL) выделяет пять процессов, составляющих преступление, связанное с торговлей людьми. Это: реклама торговцев людьми; поиск жилья и рабочих мест для пострадавших; транспортировка пострадавших; финансы; и общение между преступниками, жертвами и клиентами[583]. Каждому из этих видов деятельности способствовало развитие технологий, при этом секс-торговцы постоянно использовали их для облегчения своей преступной деятельности и эксплуатации[584]. Цифровые технологии повысили их анонимность; способствовал вербовке и эксплуатации жертв; сделал проще доступ расширить диапазоны преступной деятельности; и расширил возможности для контроля и эксплуатации жертв[585].

Вербовка через Интернет становится все более важной частью работы торговцев людьми, так как подходящие цели могут быть легко определены и с ними можно связаться[586]. Также упрощается логистика поездок и размещения – заказы и финансовые платежи могут осуществляться быстро и анонимно в режиме онлайн. Кроме того, легче общаться и координировать действия между различными компонентами и элементами, составляющими сеть трафика. Эксплуатация жертв также была облегчена благодаря Интернету: маркетинг жертв радикально изменился, и теперь большинство из них рекламируются в Интернете для более широкой аудитории и потенциальных покупателей[587]. По оценкам, 63 процента жертв торговли детьми в целях сексуальной эксплуатации рекламировались онлайн в какой-то момент.[588]

Хотя на первый взгляд это может показаться обескураживающим, киберпространство – одно из тех редких мест, где «на самом деле всплывает

преступности, резолюция 55/25 Генеральной Ассамблеи. (Ноябрь 2000 г.).
https://www.ohchr.org/Documents/ProfessionalInterest/ProtocolonTrafficking.pdf.

[583] Агентство Европейского Союза по обучению сотрудников правоохранительных органов, Торговля людьми, по состоянию на 15 февраля 2020 г.,
https://enet.cepol.europa.eu/index.php?id=online-courses&no_cache=1.

[584] Сигрид Рэтс и Джелле Янссенс, «Торговля людьми и технологии: изучение роли цифровых коммуникационных технологий в бельгийском бизнесе по торговле людьми», Европейский журнал уголовной политики и исследований, 2019 г., стр. 2, по состоянию на 20 февраля 2020 г.
https://doi.org/10.1007/s10610-019-09429-z; и Джон Ричмонд, «Уроки торговцев людьми: использование технологий для достижения основных целей движения по борьбе с торговлей людьми», речь, 8 апреля 2019 г., Миссия США при ОБСЕ, последнее изменение - 8 апреля 2019 г., по состоянию на 26 февраля 2020 г. https://osce.usmission.gov/taking-a-lesson-from-traffickers-harnessing-technology-to-f Further-the-anti-trafficking-movement/.

[585] Межведомственная координационная группа по борьбе с торговлей людьми, торговлей людьми и технологиями: тенденции, проблемы и возможности, выпуск № 7, 1, 2, 2019, по состоянию на 4 марта 2020 г., https://icat.network/sites/default/files/publications/documents/Human%20trafficking%20and%20technology%20trends%20challenges%20and%20opportunities%20WEB.pdf.

[586] Йорн ван Ридж и Рут Макалистер, «Использование преступных процедур и методов для прогнозирования и предотвращения сексуальной эксплуатации женщин из Восточной Европы в Восточной Европе», в Международном справочнике по торговле людьми Palgrave, изд. Джон Винтердик и Джеки Джонс (Palgrave Macmillan, 2020), 1693, PDF; и Raets and Janssens, «Торговля и технологии», 6.

[587] Раэтс и Янссенс, «Торговля и технологии», 8–9.

[588] «Торн, цифровые защитники детей», Институт Маккейна, по состоянию на 8 марта 2020 г., https://www.mccaininstitute.org/thorn-digital-defenders-children/.

общеизвестная тайная деятельность по торговле людьми», и некоторые из ее процессов становятся более заметными, особенно онлайн-реклама жертв[589]. Торговцы людьми в Интернете создают и оставляют цифровые следы – это следует рассматривать как данные, которые можно использовать для борьбы с ними.

Аналитика на основе ИИ

В связи с развитием торговли людьми в целях сексуальной эксплуатации в Интернете подходы к борьбе с ней все чаще основываются на данных; правоохранительным органам необходимо обрабатывать колоссальный объем данных из разрозненных источников и превращать их в полезную и действенную информацию, на которую они могут действовать[590]. Этот «постоянно растущий объем, скорость и разнообразие данных», также известный как большие данные, могут обрабатываться и анализироваться только аналитикой на основе искусственного интеллекта[591]. В этом разделе будет рассмотрено, что подразумевается под этим термином, а также как именно он используется в борьбе с торговлей людьми в целях сексуальной эксплуатации.

Аналитика на основе искусственного интеллекта – это подполе расширенной аналитики[592]. Расширенная аналитика впервые была разработана для использования в коммерческих компаниях; он определяется как «автономное или полуавтономное изучение данных или контента с использованием сложных методов и инструментов для более глубокого понимания, прогнозирования или выработки рекомендаций»[593]. Аналитика – это использование аналитических методов для обнаружения и интерпретации значимых закономерностей, корреляции и ранее невидимые связи в данных, которые люди не могли обнаружить[594].

---

[589] Раэтс и Янссенс, «Торговля и технологии», 11.

[590] Праманик М.И. и др., «Аналитика больших данных для безопасности и уголовных расследований», WIREs Data Mining и Knowledge Discovery 7, вып. 4 (июль / август 2017 г.): 1, по состоянию на 13 февраля 2020 г., https://doi.org/10.1002/widm.1208.

[591] Фергюсон, Взлет, 16.

[592] Джанет Вагнер, «Расширенная аналитика против искусственного интеллекта: чем они отличаются?», ZyloTech, https://www.zylotech.com/blog/advanced-analytics-vs.-artificial-intelligence-how-are-they-different.

[593] Gartner, цитируется в: Джереми Роуз и др., «Старт расширенной аналитики: определение, модель процесса, передовой опыт», журнал «Управление информационными системами и технологиями» 14, вып. 3 (сентябрь / декабрь 2017 г.), по состоянию на 10 февраля 2020 г., https://doi.org/10.4301/s1807-17752017000300003.

[594] Том Сабо, «Структура искусственного интеллекта для борьбы с торговлей людьми», лекция, Bright Talk, последнее изменение 5 августа 2019 г., по состоянию на 14 февраля 2020 г., https://www.brighttalk.com/webcast/17718/368329/an -Искусственный интеллект-рамки для борьбы с торговлей

В рамках расширенной аналитики есть процессы, которые управляются искусственным интеллектом и которые могут «разблокировать» больше из данных; это называется аналитикой на основе ИИ. Применяемые технологии искусственного интеллекта включают «интеллектуальный анализ данных/текста, машинное обучение, сопоставление с образцом, прогнозирование, визуализацию, семантический анализ, анализ тональности, сетевой и кластерный анализ, многомерную статистику, анализ графов, моделирование, сложную обработку событий, нейронные сети»[595]. Искусственный интеллект является одним из наиболее важных подполей в аналитике, поскольку он изменил методы интеллектуального анализа данных и, как таковой, позволяет извлекать из данных «новую эффективность и понимание», тем самым извлекая из них гораздо большую ценность, чем раньше[596].

Аналитика на основе искусственного интеллекта для борьбы с торговлей людьми

Поскольку правоохранительным органам часто не хватает инфраструктуры, ресурсов и навыков для разработки аналитических возможностей на основе ИИ, мы видим, что в этой области участники, участвующие в разработке новых технологических инициатив, разнообразны: «многоотраслевые, многопрофильные и международные»[597]. Коммерческие предприятия работают вместе с представителями государственного сектора, включая правоохранительные органы, научные круги и неправительственные организации. Правоохранительные органы, прокуратура, окружные прокуратуры и НПО по всему миру используют эти инструменты: более 30 правоохранительных органов по всему миру используют программное обеспечение Memex для помощи в расследовании случаев торговли людьми; В настоящее время Spotlight используют более 4000 сотрудников правоохранительных органов в 780 агентствах в США, что помогло выявить более 6300 жертв торговли людьми в целях сексуальной эксплуатации в США[598]; Traffic Jam имеет давние партнерские отношения с

людьми.

[595] Gartner, «Расширенная аналитика», Глоссарий Gartner.

[596] Пол Б. Саймон и Арзан Тарапор, Анализ военной разведки в эпоху больших данных, 4, 30 марта 2016 г., по состоянию на 2 марта 2020 г., https://css.ethz.ch/en/services/digital-library/articles/article.html/195263/pdf .; и Праманик и др., «Большие данные»,

[597] Надя Блисс, «На пути к конвейеру - технологии, методы и обучение», в Кодексе 8.7: Материалы конференции (Университет ООН, 2019), 13, по состоянию на 28 февраля 2020 г., https://collections.unu.edu/eserv/ УООН: 7313 / UNU_Code8.7_Final.pdf.

[598] Андреа Фокс, «3 инструмента, помогающих правоохранительным органам остановить секс-торговлю», Efficient Gov, последнее изменение 22 февраля 2017 г., по состоянию на 2 марта 2020 г., https://www.efficientgov.com/technology/articles/3-tools- помогая-правоохранительным-агентствам-остановить-

правоохранительными органами и прокуратурой. офисов и некоммерческих организаций[599].

Эти решения были разработаны специально для использования в сфере борьбы с торговлей людьми с целью сексуальной эксплуатации – они используют онлайн-связи, которые есть у покупателей и продавцов, и данные, которые это создает. Во-первых, передовые «поисковые и аналитические системы» предназначены для правоохранительных органов[600]. Затем собираются онлайн-данные, после чего множество технологий искусственного интеллекта добывают их, чтобы получить информацию, вывести закономерности, провести анализ и предоставить прогнозирует автономно[601] в «масштабе, скорости и глубине», с которыми не могут справиться специалисты-аналитики[602]. Затем он предоставляет результаты анализа в интуитивно понятных визуальных инструментах, которые помогают в принятии решений. В этой области большая часть используемых данных поступает из онлайн-рекламы сексуальных услуг.

Поисковые системы очень «ориентированы на пользователя» – они разрабатываются с учетом требований и спецификаций пользователей[603]. На основе этих требований написаны автоматизированные поисковые роботы для извлечения релевантных данных с веб-сайтов в Интернете.[604] Различные компании создают свою собственную архитектуру сканирования для отражения их потребности в данных[605]. Эти поисковые роботы просматривают миллионы онлайн-объявлений, которые содержат «чрезвычайно богатые данные», такие как изображения, номера телефонов, местоположения, рабочие имена, физические атрибуты, заголовки объявлений, цены и т. д.[606], и много других данных для сбора – по оценкам, каждый день публикуется от 400 000 до 500 000 «новых услуг для взрослых, рекламы, обзоров и обсуждений»[607].

Несмотря на огромный объем общедоступной информации, существует проблема использования всех доступных источников, поскольку рекламные объявления обычно представляют собой смесь структурированных и

секс-торговлю людьми-nq91QzbMdg3MasTS /.

[599] Броуди, «Как искусственно».

[600] Маянк Кеджривал и Педро Секели, «Следственный поиск с помощью технологий: пример из незаконного домена», Расширенные тезисы CHI'18, 2018, 2, по состоянию на 23 февраля 2020 г., https://doi.org/10.1145/3170427.3174364 .

[601] Роуз и др., «Продвинутый».

[602] Bracket Foundation, Bracket Capital, and Value for Good, Искусственный интеллект: борьба с сексуальным насилием над детьми в Интернете, 14, 2019, по состоянию на февраль 2020 г.

[603] Кеджривал и Секели, «Исследования с использованием технологий», 2.

[604] «Memex Human Trafficking Summary», DeepDive, по состоянию на 24 февраля 2020 г., http://deepdive.stanford.edu/showcase/memex.

[605] Кеджривал и Секели, «Расследование с помощью технологий».

[606] «Человек-мемекс», DeepDive.

[607] «Альянс TellFinder», TellFinder, по состоянию на 27 февраля 2020 г., https://www.tellfinder.com/ .; и Андреас Оллигшлегер (старший научный сотрудник Marinus Analytics LLC), интервью автора, онлайн, 4 февраля 2020 г.

неструктурированных данных, причем последние чрезвычайно трудоемкий сбор и добыча[608]. Кроме того, большая часть интересных данных неструктурирована и, следовательно, «скрыта» в рекламе[609]. Торговцы могут использовать Unicode, чтобы скрыть важную информацию, такую как номера телефонов или адреса[610]. Более того, чтобы избежать обнаружения, они часто размещают временные объявления или часто менять мелкие детали, такие как номера телефонов или имена в объявлениях[611]. Таким образом, недостаточно полагаться на ручной сбор и анализ, выполняемые человеком, или на базовые аналитические инструменты; ИИ может помочь выявлять и собирать важную информацию, в том числе информацию в свободной или неструктурированной форме[612].

После извлечения данные необходимо проиндексировать и каталогизировать, чтобы проанализировать их. Traffic Jam, например, создал базу данных «изображений, номеров телефонов и данных о местоположении», которая восходит к 2011 году. Благодаря тому, что сканеры очень регулярно очищают веб-сайты, объявления могут индексироваться, даже если они размещаются только временно. С 2014 по 2016 год команда MEMEX проиндексировала «80 миллионов веб-страниц и 40 миллионов изображений»[613]. В этих огромных базах данных технологии искусственного интеллекта, такие как машинное обучение, обработка естественного языка, интеллектуальный анализ текста и изображений, применяются для анализа собранной информации и получить более глубокое представление об этом явлении. Эти базы данных с терабайтами данных также можно искать по очень широким критериям. Например, можно ввести номер телефона, обнаруженный в подозрительной рекламе, и мгновенно найти другие объявления на других сайтах, связанные с тем же номером телефона.

Большинство текущих приложений включают применение технологий искусственного интеллекта, таких как машинное обучение, для выявления случаев торговли людьми с целью сексуальной эксплуатации в эскорт-рекламе и выявления сетей торговли людьми[614]. ИИ может помочь обнаружить, какие

---

[608] Педро Секели и др., «Создание и использование сети знаний для борьбы с торговлей людьми», в The Semantic Web – ISWC 2015 14-я Международная конференция по семантической паутине Вифлеем, Пенсильвания, США, 11–15 октября 2015 г., Труды, часть II, изд. . Марсело Аренас и др. (Чам: Springer, 2015), 9367: 206; и Роуз и др., «Расширенная аналитика».

[609] Рената А. Конрад и др., «Преодоление торговли людьми с помощью операционных исследований и аналитики: возможности для методов, моделей и приложений», Европейский журнал операционных исследований 259, вып. 2 (1 июня 2017 г.): 738, по состоянию на 3 марта 2020 г., https://doi.org/10.1016/j.ejor.2016.10.049.

[610] Секели и др., «Строительство и использование», 9367: 206.

[611] Конрад и др., «Преодолевая человека», 735.

[612] Kackenmeister, «AI и борьба», Университет Лихай.

[613] Анастасия Менсикова и Крис А. Маттманн, «Ансамблевой анализ настроений для выявления торговли людьми в веб-данных», GTA3 2018, февраль 2018, 1, по состоянию на 5 марта 2020 г., https://doi.org/10.475/123_4.

[614] Ребекка С. Портнофф и др., «Backpage and Bitcoin: Uncovering Human Traffickers», KDD 2017, 2017, 1596, по

объявления отображают людей, ставших жертвами торговли людьми, путем обнаружения «поведенческих сигналов в Интернете» в рекламе», которые указывают на то, что это лицо могло быть продано. Рекламные объявления можно анализировать с помощью методов интеллектуального анализа данных, которые полагаются на визуальные подсказки, например, если татуировки присутствуют на нескольких изображениях; или текстовые подсказки, включая «особые стили написания рекламы; ключевые слова и т.д.» чтобы помочь отличить подозрительную рекламу от не подозрительной[615]. Еще одна ключевая задача расширенной аналитики на основе ИИ – «группировать рекламу по истинному владельцу», а не по заявленным авторам[616]. Разрешение сущности предполагает обнаружение ИИ «набора явных связей между объектами, извлеченных из разных источников»[617]. В результате такие объекты, как номера телефонов и адреса электронной почты, могут использоваться для поиска шаблонов и подключения разнородных рекламных объявлений, которые, скорее всего, написаны одними и теми же торговцами в разных географических регионах[618]. Это известно как запись связь и позволяет правоохранительным органам идентифицировать одну и ту же сущность, на которую ссылаются в разных источниках и в разное время[619]. Некоторые программы, включая Traffic Jam и XIX, также полагаются на возможности анализа изображений – эти инструменты могут очищать изображения или идентифицировать похожие фотографии, которые появляются в отключенной рекламе[620]. Traffic Jam также использует программное обеспечение для распознавания лиц для идентификации жертв торговли людьми – правоохранительные органы могут выставить фотографию пропавшего без вести на фоне других ее фотографии в базе данных, чтобы помочь определить, рекламируется ли человек в Интернете[621]. Наконец, аналитика на основе ИИ также может помочь выявить критические ссылки и узлы в сети и ее структуре. Впоследствии можно выявить наиболее ценные модели и тенденции, такие как значимые отношения, ключевые люди в ядре сети и потоки между узлами (например, товаров, финансов или информации).

Дополнительная ценность данных может быть получена за счет инновационной визуализации данных и информации, полученной в результате

состоянию на 5 марта 2020 г. https://doi.org/10.1145/3097983.3098082.

[615] Раэтс и Янссенс, «Торговля и технологии», 13; и Менсикова и Маттманн, «Ансамблевые настроения», 1.

[616] Portnoff et al., «Backpage and Bitcoin», 1596, курсив добавлен автором.

[617] Секели и др., «Строительство и использование», 9367: 215.

[618] Секели и др., «Строительство и использование», 9367: 2047, 215; и Raets and Janssens, «Торговля и технологии»,

[619] Кайл Россетти и Ребекка Билбро, «Основы разрешения проблем с помощью Python и Dedupe», District Data Labs, по состоянию на 3 марта 2020 г.,
https://www.districtdatalabs.com/basics-of-entity-resolution.

[620] Шон Капитан, «Этот ИИ может обнаруживать признаки торговли людьми в секс-рекламе в Интернете», Fast Company, 4 ноября 2019 г., по состоянию на 6 марта 2020 г.
https://www.fastcompany.com/90424645/how-image-recognition-ai-is-busting-sex-traffickers.

[621] Касер, «Эта компания», The Next Web.

анализа. Построение целостного и контекстуального понимания торговли людьми на основе потока данных основаных на визуализации зданий искусственного интеллекта, таких как интерактивные пользовательские интерфейсы, информационные панели, графики, матрицы тепловых карт, «искровые линии для отображения временных колебаний» или карты со стрелками, указывающими разные города, в которых рекламируется один и тот же номер телефона[622]. Аналитическая визуализация позволяет офицерам более эффективно реагировать на данные, поскольку соответствующие выводы становятся более интуитивно понятными для чтения и понимания, и, таким образом, можно принимать более обоснованные решения[623]. Этот инструмент визуализации также очень важен при передаче результатов в органы управления и лица, принимающие решения, которым может не хватать предметных знаний[624].

Оценка

В целом, аналитика на основе искусственного интеллекта помогает следователям: находить объявления, которые, скорее всего, будут рекламировать людей, ставших предметом торговли; разъяснение привычек и структуры организаций торговли людьми; уделение первоочередного внимания ограниченным ресурсам правоохранительных органов; и выявление возможных и наиболее эффективных вмешательств[625]. Важно подчеркнуть, что аналитика, основанная на искусственном интеллекте, не исключает людей из борьбы с торговлей людьми. Напротив, эта технология в основном используется для создания следственных действий, при этом «человеческий интеллект и принятие решений» по-прежнему необходимы для принятия мер[626]. Действительно, когда рекламные объявления выделяются как потенциально связанные с торговлей людьми, это все еще зависит от агентов-людей. Пересмотрите классификацию, решите, как и где действовать и как распределять ресурсы. То, что мы наблюдаем, представляет собой «тандем» между традиционными методами и новыми технологиями, которые помогают правоохранительным органам[627]. Основываясь на этом обзоре технологии в

---

[622] Майорга и др., «Противодействие человеку», 248.
[623] Марко Аннунциата, «ИИ и визуализация данных: как ИИ помогает компаниям видеть сквозь туман данных», Forbes, 9 февраля 2019 г., по состоянию на 1 марта 2020 г., https://www.forbes.com/sites/marcoannunziata/2019 / 02/09 / ai-and-data-visualization-how-ai-help-companies-see-through-the-fog-of-data / # 73268a7f7cf3
[624] Давина Дургана, «Данные правительства горнодобывающей промышленности для достижения цели 8.7», в Кодексе 8.7: Материалы конференции (Университет ООН, 2019), 6, по состоянию на 2 марта 2020 г., https://collections.unu.edu/eserv/UNU: 7313 / UNU_Code8.7_Final.pdf
[625] «Человек-мемекс», DeepDive.
[626] Основание скобок, Капитал скобок и ценность во благо, Искусственный интеллект, 20.
[627] Раэтс и Янссенс, «Торговля и технологии», 18.

применении к расследованиям торговли людьми в целях сексуальной эксплуатации, в этом разделе будут оцениваться три значительных воздействия аналитики на основе ИИ на правоохранительные органы.

Более активные ответы

Выявляя идеи и связи на основе данных, которые в противном случае не были бы обнаружены, аналитика на основе ИИ меняет сам подход офицеров к расследованию сексуальных преступлений. Этот новый подход к борьбе с преступностью получил название «полицейская деятельность на основе данных», и он включает автоматический сбор и анализ больших наборов данных, в данном случае с помощью аналитики, управляемой ИИ, что позволяет полицейским формировать свои меры и реагировать на основе информации в реальном времени[628].

Обладая большей информацией, правоохранительные органы лучше понимают, какие выводы являются более важными и как следует расставлять приоритеты ограниченным ресурсам[629]. Автоматизация также играет ключевую роль в сокращении времени, необходимого для проведения расследований и операций[630]. Это не только высвобождает невероятное количество ресурсов. Офицерам нужно время, чтобы сосредоточиться на других ключевых задачах, но это также увеличивает количество расследований, которые можно провести, вероятно, увеличивая количество спасенных жертв. Например, XIX может составить отчет разведки для правоохранительных органов за шесть часов вместо предыдущих 22 дней[631], а окружной прокурор Манхэттена смог увеличить количество расследований торговли людьми, которые они проводят ежегодно, с 30 до 300 с момента работы с аналитическим программным обеспечением на основе искусственного интеллекта[632].

Более того, информация в режиме реального времени позволяет сотрудникам разрабатывать более «целенаправленные вмешательства» и иметь гораздо более активный подход к работе полиции[633]. Визуализация различных звеньев, составляющих сеть торговли людьми, позволяет сотрудникам правоохранительных органов разрабатывать операции, которые блокируют важные потоки между торговцами людьми, или нацеливать на критически

---

[628] https://cops.usdoj.gov/RIC/Publications/cops-w0558-pub.pdf; и Фергюсон, Восстание.
[629] Бабута, Освальд и Джанжева, Искусственный интеллект, 7.
[630] Фергюсон, Взлет, 103.
[631] Капитан, «Этот ИИ может заметить».
[632] Броуди, «Как искусственно».
[633] Код 8.7: Материалы конференции (Университет Организации Объединенных Наций, 2019 г.), 11, по состоянию на 7 марта 2020 г., https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

важные субъекты, которые в случае устранения могут дестабилизировать или привести к краху сети[634]. Кроме того, они могут организовать операции, нацеленные на других участников, которые «создают, содействуют и увековечивают» торговлю людьми с целью сексуальной эксплуатации, таких как финансовые спонсоры, клиенты, рекрутеры и и так далее[635]; и обнаруживая маршруты торговли людьми, методы транспортировки, убежища и горячие точки вербовки, легче спланировать быстрые операции, которые могут спасти жертв в этих точках[636]. Наконец, понимание потоков, а также временных и географических моделей торговля людьми имеет решающее значение для выработки адаптированных и решительных ответных мер. Например, данные Traffic Jam помогли опровергнуть распространенное мнение о росте торговли людьми до и во время таких событий, как Суперкубок[637]. Эти знания не позволяют правоохранительным органам неправильно использовать ограниченные ресурсы во время подобных событий.

Повышенное доверие правоохранительных органов к данным

С продолжающимся производством цифровых данных и преимуществами, которые дает подход, основанный на данных, кажется вероятным, что использование правоохранительными органами аналитики на основе ИИ станет только шире. Однако это имеет определенные ограничения. Эта технология зависит от больших и точных наборов данных; тем не менее, существуют значительные «пробелы в данных»[638]. Данные о «распределении жертв, торговцев людьми, покупателей и эксплуататоров» часто ненадежны или частичны.[639] Кроме того, существуют пробелы в знаниях о потоках торговли людьми в больших частях мира, таких как области в Африке и на Ближнем Востоке, и оценки в основном основаны на неметодических или неполных данных, основанных только на зарегистрированных случаях[640]. Это рисует неточную картину «характера и масштабов» торговли людьми во всем мире,

---

[634] Фаррелл и де Фрис, «Измерение природы», 157.

[635] Розальва Ресендис и Лукас Э. Эспиноза, «Международное правоохранительное сообщество: совместные усилия в борьбе с торговлей людьми», в Справочнике SAGE по торговле людьми и современному рабству, под ред. Дженнифер Брайсон Кларк и Саша Поуки (Sage, 2019), 480, по состоянию на 12 февраля 2020 г.

[636] Конрад и др., «Преодолевая человека», 737.

[637] Александра Оссола, «Инструмент искусственного интеллекта помогает правоохранительным органам находить жертв торговли людьми», Futurism, 16 апреля 2018 г., по состоянию на 5 марта 2020 г., https://futurism.com/ai-tool-law-enforcement-stop-human- торговля людьми.

[638] Фергюсон, Взлет, 184.

[639] Конрад и др., «Преодолевая человека», 736.

[640] ЮНОДК, Глобальный отчет, 15.

тем самым препятствуя глобальным рамкам и ответные меры, предусмотренные сообществом по борьбе с торговлей людьми[641].

Более того, поскольку «при сборе больших данных не учитываются те, кого он не видит»[642], полагаясь на данные, правоохранительные органы вынуждены действовать только в отношении преступлений, которые в определенный момент создают онлайн-данные. Торговля людьми в целях сексуальной эксплуатации, возможно, является одним из преступлений, с которыми лучше всего бороться с помощью усилий, основанных на данных, благодаря размещаемой торговцами онлайн-рекламе[643]. Тем не менее, они составляют лишь часть всей цепочки торговли людьми в целях сексуальной эксплуатации; большая его часть остается невидимой, создавая мало данных и, следовательно, мало информации, на которую можно воздействовать. Более того, использование данных также представляет угрозу безопасности, поскольку преступники могут обнаружить, как лучше скрыть свои данные и сделать их непригодными для использования; или они могут изменять данные, чтобы дезинформировать правоохранительные органы.

ИИ как черный ящик

Правоохранительные органы часто не имеют собственной инфраструктуры, ресурсов или навыков для разработки расширенных аналитических возможностей на основе ИИ[644]. Поэтому представляется вероятным, что текущая коммерческая модель, согласно которой частные компании разрабатывают инструменты, которые они передают правоохранительным органам не изменится. Однако это вызывает некоторые опасения, поскольку программное обеспечение часто является проприетарным и отсутствует прозрачность в отношении того, как были созданы алгоритмы и как они работают[645].

Один из рисков заключается в том, что частные компании разрабатывают системы искусственного интеллекта, известные как «черные ящики». Это относится к случаям, когда из-за сложности технологии методы обработки данных систем ИИ непрозрачны и могут быть непонятны операторам[646].

---

[641] Фаррелл и де Вриз, «Измерение природы», 148.
[642] Фергюсон, Взлет, 185.
[643] Раэтс и Янссенс, «Торговля и технологии», 11.
[644] Искусственный интеллект, 24.
[645] Рэнди Риланд, «Искусственный интеллект теперь используется для прогнозирования преступлений. Но является ли это предвзятым? », Smithsonian Magazine, 5 марта 2018 г., по состоянию на 7 марта 2020 г., https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it -смещенный-180968337 /
[646] Александр Бабута, Марион Освальд и Кристин Риник, Алгоритмы машинного обучения и принятие решений

Отсутствие интерпретируемости может привести к закону.

Сотрудники правоохранительных органов не могут объяснить доказательства, полученные против подозреваемых торговцев людьми в ходе судебных дел, что может подорвать «прозрачность всего процесса отправления правосудия»[647] и помешать осуждению за торговлю людьми с целью сексуальной эксплуатации.[648] Кроме того, алгоритмы и наборы данных, на которых они основаны, редко подвергаются проверке, что потенциально позволяет внедрить предвзятость в программы[649]. Для того, чтобы сотрудники полиции сохраняли ответственность за окончательное принятие решений, необходимо, чтобы системы были спроектированы таким образом, чтобы «пользователи, не имеющие технической квалификации, могли интерпретировать и критически оценивать ключевую техническую информацию».[650]

Несмотря на этот риск, Бабута, Освальд и Риник подчеркивают, что мультидисциплинарный характер партнеров, участвующих в разработке таких программ, может фактически снизить риск разработки и внедрения предвзятых и непрозрачных алгоритмов. Такая задача связана с «техническими, организационными и правовыми сложностями», и предполагается, что межотраслевое партнерство является способом решения всех этих сложностей.[651] Кроме того, многие компании, участвующие в сообществе по борьбе с торговлей людьми, были разработка программного обеспечения с открытым исходным кодом – тенденция, которая может смягчить эффект черного ящика.

Тем не менее, необходимо создать более широкую и всеобъемлющую основу для руководства этими усилиями и более широким распространением технологий искусственного интеллекта в правоохранительных органах. Установление этических и правовых норм является первостепенной задачей, но необходимо также учитывать, как подготовка сотрудников правоохранительных органов должна развиваться, чтобы отражать эти изменения. Офицеры должны быть в состоянии понимать технологии ИИ и работать с ними прозрачным и понятным образом; но они также должны быть в курсе последних технологических инноваций, чтобы понимать, как они могут практически повлиять на правоохранительные органы. Полный спектр

полицией: правовые, этические и нормативные проблемы, отчет № 3-18, 17 сентября 2018 г., по состоянию на 9 марта 2020 г.,
https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf

[647] Бабута, Освальд и Риник, Машинное обучение, 17.

[648] Олигшлегер, интервью автора.

[649] Рональд Ю и Габриэле Спина Али, «Что внутри черного ящика? Проблемы искусственного интеллекта для юристов и исследователей »,« Управление правовой информацией », 19, вып. 1 (март 2019 г.): по состоянию на 2 марта 2020 г., https://doi.org/10.1017/S1472669619000021.

[650] Бабута, Освальд и Джанжева, Искусственный интеллект, viii.

[651] Бабута, Освальд и Риник, Машинное обучение, 27.

последствий внедрения ИИ в систему уголовного правосудия еще не был полностью спрогнозирован[652], и хотя преимущества многочисленны, этот обзор также продемонстрировал, что важные ограничения сохраняются, и их следует продолжать отслеживать, поскольку технологии ИИ более широко используется правоохранительными органами.

Вывод

Технологии преобразовали и изменили конфигурацию торговли людьми в целях сексуальной эксплуатации, но также и усилия по борьбе с торговлей людьми: с преобладанием доступных данных был принят более проактивный и основанный на данных подход полиции. Аналитика на основе искусственного интеллекта – особенно важная технология, которая может анализировать большие наборы данных и генерировать ценную информацию и полезные сведения для правоохранительных органов.

Это пример плодотворного партнерства между технологиями и противодействием торговле людьми. Его применение для борьбы с торговлей людьми в целях сексуальной эксплуатации оказывает конкретное и положительное влияние на то, как правоохранительные органы могут бороться с этим преступлением. Однако использование этой технологии влияет не только на создание программного обеспечения, но и на саму концепцию борьбы с преступностью – на стыке технологий и данных. Следует ожидать, что передовые аналитические инновации, основанные на искусственном интеллекте, будут продолжать распространяться и станут незаменимым инструментом для правоохранительных органов. Таким образом, необходимо понимать не только технологию, но и принимать во внимание более широкий контекст, в котором она работает, например, правовой и социальный. Необходимо создать всеобъемлющую основу для использования передовой аналитики искусственного интеллекта в правоохранительных органах; и хотя применение аналитики на основе искусственного интеллекта теперь предназначено исключительно для расследований торговли людьми с целью сексуальной эксплуатации, могут появиться новые возможности использования ранее непригодных для использования данных и расширения этих технологий для борьбы с другими видами торговли людьми или преступностью в целом.

[652] Бабута, Освальд и Риник, Машинное обучение, 10.

Ссылки

Аннунциата, Марко. «Искусственный интеллект и визуализация данных: как ИИ помогает компаниям видеть сквозь туман данных». Forbes, 9 февраля 2019 г. По состоянию на 1 марта 2020 г. https://www.forbes.com/sites/marcoannunziata/2019/02/09/ai-and-data-visualization-how-ai-helps-companies-see -через-туман-данных / # 73268a7f7cf3.

Искусственный интеллект и робототехника для правоохранительных органов. Интерпол|UNICRI, 2019. https://issuu.com/unicri/docs/artificial_intelligence_robotics_la/1?ff.

Бабута, Александр, Марион Освальд и Арди Джанджева. Искусственный интеллект и национальная безопасность Великобритании: соображения политики. Королевский институт объединенных служб, 2020. https://rusi.org/sites/default/files/ai_national_security_final_web_version.pdf.

Бабута, Александр, Марион Освальд и Кристин Риник. Алгоритмы машинного обучения и принятие решений в полиции: правовые, этические и нормативные проблемы. № отчета 3-18. Сентябрь 2018 г. По состоянию на 9 марта 2020 г.

https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf.

Блаженство, Надя. «К трубопроводу - технологии, методы и обучение». В Кодексе 8.7: Материалы конференции, 12-13. Университет Организации Объединенных Наций, 2019. По состоянию на 28 февраля 2020 г. https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

Бозе, Ранджит. «Расширенная аналитика: возможности и проблемы». Промышленные системы управления и данных 109, вып. 2 (2009): 155-72.

https://doi.org/10.1108/02635570910930073.

Основание кронштейна, капитал кронштейна и ценность во благо. Искусственный интеллект: борьба с сексуальным насилием в отношении детей в Интернете. 2019.

По состоянию на февраль 2020 г. https://www.flipbookpdf.net/web/files/uploads/765c57681ad3259906107226b5934880ca9dbebfFBP17764427.pdf.

Броуди, Лиз. «Как искусственный интеллект отслеживает лиц, занимающихся секс-торговлей». OneZero, 8 мая 2019 г., дата обращения 11 марта 2020 г.

https://onezero.medium.com/how-artificial-intelligence-is-tracking-sex-traffickers-276dcc025ecd.

Капитан, Шон. «Этот ИИ может обнаруживать признаки торговли людьми в секс-рекламе в Интернете». Fast Company, 4 ноября 2019 г., дата обращения 6 марта 2020 г.

https://www.fastcompany.com/90424645/how-image-recognition-ai-is-busting-sex-traffickers.

Кокейн, Джеймс. «Создание стимулов для действий - исследования, регулирование и вознаграждения». В Кодексе 8.7: Материалы конференции, 14-15. Университет Организации Объединенных Наций, 2019. По состоянию на 11 марта 2020 г. https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

Дубравски, Артур, Кайл Миллер, Мэтью Барнс, Бенедикт Бекинг и Эмили Кеннеди. «Использование общедоступных данных для выявления моделей деятельности по торговле людьми». Журнал торговли людьми 1, вып. 1 (2015): 65-85. По состоянию на 12 марта 2020 г.

https://doi.org/10.1080/23322705.2015.1015342.

Дуонг, Ким Ань. «Комплексная гендерная структура для оценки политики и программ по борьбе с торговлей людьми». В Международном справочнике по торговле людьми Палгрейв, под редакцией Джона Винтердака и Джеки Джонса, 247–69. Пэлгрейв Макмиллан, 2020. PDF.

Дургана, Давина. «Данные правительства горнодобывающей промышленности для достижения цели 8.7». В Кодексе 8.7: Материалы конференции, 5-6. Университет Организации Объединенных Наций, 2019. По состоянию на 2 марта 2020 г. https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

Агентство Европейского Союза по обучению сотрудников правоохранительных органов. Торговля людьми. По состоянию на 15 февраля 2020 г. https://enet.cepol.europa.eu/index.php?id=online-courses&no_cache=1.

Фаррелл, Эми и Ике де Фриз. «Измерение характера и распространенности торговли людьми». В Международном справочнике по торговле людьми Палгрейв, под редакцией Джона Винтердака и Джеки Джонса, 147–62. Пэлгрейв Макмиллан, 2020. PDF.

Фергюсон, Эндрю Гатри. Рост полицейской службы больших данных: наблюдение, гонка и будущее правоохранительных органов. Нью-Йорк: Издательство Нью-Йоркского университета, 2017.

Фокс, Андреа. «3 инструмента, помогающих правоохранительным органам остановить секс-торговлю». Эффективное правительство Последнее изменение: 22 февраля 2017 г. По состоянию на 2 марта 2020 г. https://www.efficientgov.com/technology/articles/3-tools-helping-law-enforcement-agencies-stop-sex-trafficking-nq91QzbMdg3MasTS/ .

Gartner. «Расширенная аналитика». Глоссарий Gartner. Доступ 24 января 2020 г.

https://www.gartner.com/en/information-technology/glossary/advanced-analytics.

Хоанг, Тхи. Решение проблемы завтрашнего рабства сегодня.

Составлено УВКПЧ. Проверено 9 марта 2020 г.

https://www.ohchr.org/Documents/Issues/Slavery/SR/AddressingTomorrowSlaveryToday/TechnologyAgainstTrafficking.pdf.

Межведомственная координационная группа по борьбе с торговлей людьми.

Торговля людьми и технологии: тенденции, проблемы и возможности.

Краткий выпуск № 7. 2019. По состоянию на 4 марта 2020 г. https://icat.network/sites/default/files/publications/documents/Human%20trafficking%20and%20technology%20trends%20challenges%20and%20opportunities%20WEB....pdf .

Джонс, Пол и Хлоя Сеттер. «Поиск скрытых групп населения - торговля сиротами».

В коде 8.7: Материалы конференции, 10-11. Университет Организации Объединенных Наций, 2019.

По состоянию на 7 марта 2020 г. https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

Kackenmeister, Кэти. «AI и борьба с торговлей людьми». Лихайский университет. Последнее изменение 30 октября 2019 г. Проверено 3 марта 2020 г. https://engineering.lehigh.edu/news/article/ai-and-fight-against-human-trafficking.

Касер, Рэйчел. «Эта компания использует распознавание лиц для борьбы с торговлей людьми». Следующая Сеть. Последнее изменение 1 июня 2018 г. Проверено 9 марта 2020 г. https://thenextweb.com/world/2018/06/01/this-company-is-using-facial-recognition-to-fight-human-trafficking/.

Кеджривал, Маянк и Педро Секели. «Следственный поиск с использованием технологий: пример из незаконной области». Расширенные

тезисы CHI'18, 2018, 1-9. По состоянию на 23 февраля 2020 г. https://doi.org/10.1145/3170427.3174364.

Конрад, Рената А., Эндрю С. Трапп, Тимоти М. Палмбах и Джеффри С. Блом. «Преодоление торговли людьми с помощью операционных исследований и аналитики: возможности для методов, моделей и приложений». Европейский журнал операционных исследований 259, вып. 2 (1 июня 2017 г.): 733-45. По состоянию на 3 марта 2020 г. https://doi.org/10.1016/j.ejor.2016.10.049.

Ландман, Тодд. «Картирование и моделирование уязвимостей». В Коде 8.7:

Отчет о конференции, 1-2. Университет Организации Объединенных Наций, 2019. По состоянию на 3 марта 2020 г. https://collections.unu.edu/eserv/UNU:7313/UNU_Code8.7_Final.pdf.

Левенталь, Барри. «Введение в интеллектуальный анализ данных и другие методы расширенной аналитики». Журнал практики прямого, информационного и цифрового маркетинга 12, вып. 2 (2010): 137-53.

Майорга, Мария, Лаура Татеосян, Герман Веласкес, Реза Аминдарбари и Шерри Кальтаджироне. «Противодействие торговле людьми с использованием методов ISE / OR».

В Emerging Frontiers in Industrial and Systems Engineering: Success через Collaboration, под редакцией Харриет Б. Нембхард, Элизабет А. Кадни и Кэтрин М. Коперич, 237-57. CRC Press, 2019. PDF.

«Сводка по торговле людьми Memex». Глубокое погружение. По состоянию на 24 февраля 2020 г. http://deepdive.stanford.edu/showcase/memex.

Менсикова, Анастасия и Крис А. Маттманн. «Комплексный анализ настроений

для выявления торговли людьми в веб-данных». GTA3 2018, 1-6 февраля 2018 г.

По состоянию на 5 марта 2020 г. https://doi.org/10.475/123_4.

Оллигшлэгер, Андреас (старший научный сотрудник Marinus Analytics LLC).

Интервью автора. В сети. 4 февраля 2020 г.

Оссола, Александра. «Инструмент ИИ помогает правоохранительным органам находить жертв торговли людьми». Футуризм, 16 апреля 2018 г. По состоянию на 5 марта 2020 г.

https://futurism.com/ai-tool-law-enforcement-stop-human-trafficking.

Пеллерин, Шерил. «Программа DARPA помогает бороться с торговлей людьми».

Оборона. Последнее изменение 4 января 2017 г. Проверено 4 марта 2020 г.

https://www.defense.gov/Explore/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/.

Портнофф, Ребекка С., Дэнни Юсин Хуанг, Барвинк Дёрфлер, Садия Афроз и Дэймон Маккой. «Backpage и биткойн: раскрытие торговцев людьми». КДД 2017, 2017, 1595-604.

По состоянию на 5 марта 2020 г. https://doi.org/10.1145/3097983.3098082.

Праманик, М.И., Раймонд Ю.К. Лау, Вэй Т. Юэ, Юньмин Е и Чунпин Ли. «Аналитика больших данных для безопасности и уголовных расследований». WIREs Data Mining и Knowledge Discovery 7, no. 4 (июль / август 2017 г.): 1-19. По состоянию на 13 февраля 2020 г. https://doi.org/10.1002/widm.1208.

Протокол о предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее, дополняющий Конвенцию Организации Объединенных Наций против транснациональной организованной преступности, резолюция 55/25 Генеральной Ассамблеи. (Ноябрь 2000 г.).

https://www.ohchr.org/Documents/ProfessionalInterest/ProtocolonTrafficking.pdf.

Раэтс, Сигрид и Джелле Янссенс. «Торговля людьми и технологии: изучение роли цифровых коммуникационных технологий в бельгийском бизнесе по торговле людьми». Европейский журнал уголовной политики и исследований, 2019, 1-24. Доступ 20 февраля 2020 г.

https://doi.org/10.1007/s10610-019-09429-z.

Ресендиз, Розальва и Лукас Эспиноза. «Международное правоохранительное сообщество: совместные усилия в борьбе с торговлей людьми». В Справочнике SAGE по торговле людьми и современному рабству под редакцией Дженнифер Брайсон Кларк и Саши Поуки, 469–85. Sage, 2019. По состоянию на 12 февраля 2020 г.

Ричмонд, Джон. «Уроки торговцев людьми: использование технологий для достижения основных целей движения по борьбе с торговлей людьми». Выступление, 8 апреля 2019 г. Миссия США при ОБСЕ. Последнее изменение 8 апреля 2019 г. Проверено 26 февраля 2020 г.

https://osce.usmission.gov/taking-a-lesson-from-traffickers-harnessing-technology-to-f Further-the-anti-trafficking-movement/.

Риланд, Рэнди. «Искусственный интеллект теперь используется для прогнозирования преступлений. Но предвзято ли это? » Smithsonian Magazine, 5 марта 2018 г. По состоянию на 7 марта 2020 г. https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/.

Роуз, Джереми, Микаэль Берндтссон, Гуннар Матиасон и Питер Ларссон. «Старт Advanced Analytics: определение, модель процесса, передовой опыт». Журнал информационных систем и управления технологиями 14, вып. 3 (сентябрь / декабрь 2017 г.). Доступ 10 февраля 2020 г.

https://doi.org/10.4301/s1807-17752017000300003.

Россетти, Кайл и Ребекка Бильбро. «Основы разрешения сущностей с помощью Python и Dedupe». Районные лаборатории данных. Доступ 3 марта 2020 г.

https://www.districtdatalabs.com/basics-of-entity-resolution.

Сабо, Том. «Система искусственного интеллекта для борьбы с торговлей людьми».

Лекция. Яркий разговор. Последнее изменение 5 августа 2019 г. Дата доступа 14 февраля 2020 г. https://www.brighttalk.com/webcast/17718/368329/an-artificial-intelligence-framework-to-combat-human-trafficking.

Саймон, Пол Б. и Арзан Тарапор. Анализ военной разведки в эпоху больших данных.

30 марта 2016 г. Проверено 2 марта 2020 г.

https://css.ethz.ch/en/services/digital-library/articles/article.html/195263/pdf.

Секели, Педро, Крэйг А. Ноблок, Джейсон Слепика, Эндрю Филбот, Амандип Сингх, Ченге Инь, Дипси Капур, Прем Натараджан, Даниэль Марку, Кевин Найт, Дэвид Сталлард, Subessware

С. Карунамурти, Раджагопал Боджанапалли, Стивен Минтатулли, Стивен Минтатулли, Тодд Хьюз, Майк Тамайо, 81 год

Дэвид Флинт, Рэйчел Артисс, Ши-Фу Чанг, Тао Чен, Джеральд Хибель и Лидия Феррейра. «Создание и использование сети знаний для борьбы с торговлей людьми». В The Semantic Web – ISWC 2015 14-я Международная конференция по семантической паутине Вифлеем, Пенсильвания, США, 11–15 октября 2015 г. Труды, часть II, под редакцией Марсело Аренаса, Оскара Корчо, Елены Симперл, Маркуса Стромайера, Матье д'Аквина, Кавиты Сринивас, Пол Грот, Мишель Дюмонтье, Джефф Хефлин, Кришнапрасад Тирунараян и Штеффен Стааб, 205–21. Vol. 9367. Чам: Springer, 2015.

Таринелли, Райан. «Спустя несколько месяцев после закрытия Backpage» секс-реклама в Интернете возобновляется. National Post (Даллас), 28 ноября 2018 г. По состоянию на 12 марта 2020 г. https://nationalpost.com/pmn/news-pmn/online-sex-ads-rebound-months-after-shutdown-of-backpage.

«Альянс TellFinder». TellFinder. По состоянию на 27 февраля 2020 г. https://www.tellfinder.com/.

«Торн, цифровые защитники детей». Институт Маккейна. По состоянию на 8 марта 2020 г. https://www.mccaininstitute.org/thorn-digital-defenders-children/.

УНП ООН. Глобальный отчет о торговле людьми, 2018 г., декабрь 2018 г. По состоянию на 11 февраля 2020 г.

https://www.unodc.org/documents/dataalysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf.

ван Ридж, Йорн и Рут Макалистер. «Использование преступных процедур и методов для прогнозирования и предотвращения сексуальной эксплуатации восточноевропейских женщин в Восточной Европе». В Международном справочнике по торговле людьми Палгрейва, под редакцией Джона Винтердака и Джеки Джонса, 1689-708. Пэлгрейв Макмиллан, 2020. PDF.

Вагнер, Джанет. «Расширенная аналитика против искусственного интеллекта: чем они отличаются?» ZyloTech.

https://www.zylotech.com/blog/advanced-analytics-vs.-artificial-intelligence-how-are-they-different.

Винтердик, Джон и Джеки Джонс, ред. Международный справочник Palgrave по торговле людьми. Пэлгрейв Макмиллан, 2020. PDF.

Ю, Рональд и Габриэле Спина Али. «Что внутри черного ящика? Проблемы искусственного интеллекта для юристов и исследователей ». Управление правовой информацией 19, вып. 1 (март 2019): 2-13. По состоянию на 2 марта 2020 г. https://doi.org/10.1017/S1472669619000021.

8. Режимы данных: аналитическое руководство для понимания, как правительства регулируют данные

Хантер Дорварт * и Елена Михальченко **[653]

Искусственный интеллект (ИИ) ставит новые проблемы для эффективного управления данными на местном, национальном и международном уровнях. Учитывая разнообразие исторических, культурных и институциональных структур между национальными государствами, правительства во всем мире начинают расходиться в том, как они регулируют экосистему больших данных и утверждают власть над цифровой сферой. Отсутствие последовательной основы для анализа этих различных подходов к управлению данными препятствовало гармонизации национальных интересов и препятствовало усилиям международных организаций по созданию четких обязательств в отношении возникающих технологических проблем, таких как AI, цифровое наблюдение и трансграничные потоки данных. Мы утверждаем, что такая гармонизация необходима для обеспечения соответствия новых технологий нормам прав человека, предотвращения балканизации цифровой сферы и создания полицейских государств. В этом документе вводится новый термин – режим данных – для устранения этого недостатка и лучшего понимания возникающей фрагментации цифрового пространства, предлагая новую структуру классификации того, как государства отстаивают свою власть над цифровыми технологиями и Интернетом. Режим данных охватывает не только инструменты политики, которые страны используют для достижения своих целей в отношении технологий, но также то, как эти инструменты соотносятся с более крупными нормативными ценностями, которые определяют глобальное взаимодействие между государствами. Наконец, помогая в выявлении национальных интересов в области данных, структура кодифицирует новый взгляд на международное управление данными.

---

[653] * Хантер Дорварт в настоящее время является независимым исследователем, проживающим в Вашингтоне, округ Колумбия, который сотрудничал с многочисленными организациями в области технологической политики, включая Ассоциацию индустрии телекоммуникаций (TIA) и Международную ассоциацию адвокатов (IBA).

** Елена Михальченко - опытный адвокат по правам человека, специализирующийся на взаимосвязи права и технологий. После учебы в США в качестве стипендиата программы Фулбрайта и Эдмунда С. Маски она стала научным сотрудником Института Портуланса, где изучает возникающие проблемы управления Интернетом и технологий.

Четвертая промышленная революция относится к прогнозируемым повсеместным экономическим и социальным изменениям, вызванным новыми технологиями, которые объединяют физическую, цифровую и биологическую сферы в единый производственный процесс. Ученые связывают этот термин с предыдущими революциями в человеческой организации, которые привели к глубоким преобразованиям в фундаментальных способах функционирования общества и использования технологий. Видеть. Тессалено Девезас и др. Индустрия 4.0: предпринимательство и структурные изменения в новом цифровом ландшафте (2016 г.); Клаус Шваб. Четвертая промышленная революция, (2016).

Ключевые слова: данные, искусственный интеллект, управление данными, экосистема данных, конфиденциальность данных.

Вступление

Тенденция фрагментации, которая подчеркивает процесс глобализации, вероятно, усилится, поскольку страны продолжают бороться с множеством проблем управления. Такие проблемы сейчас касаются многих областей, включая фискальную и денежную нестабильность, поверхностные экономические прогнозы, демографические и миграционные проблемы, уязвимость цепочки поставок, экологические проблемы и кризисы в области общественного здравоохранения. Действительно, поскольку правительства преследуют свои собственные национальные интересы в условиях растущего внутриполитического давления, совместное участие в международный домен охотно уступает место конкурентной ретракции.

Одна из таких областей фрагментации касается цифрового пространства и глобального Интернета. В ответ на новые технологические тенденции, такие как «Четвертая промышленная революция» и искусственный интеллект (ИИ), правительства расходятся во мнениях относительно того, как они регулируют данные, устанавливают контроль над цифровыми процессами и управляют взаимосвязанными системами связи. Действительно, ситуация создает конфликт. сценарии будущих правил цифрового пространства и нормативных ценностей, которые определяют глобальное взаимодействие[654]. Если не рассматривать эти сценарии осмысленным образом, они грозят вызвать еще большую нестабильность и повысить риски, связанные с современными тенденциями, такими как экологическая катастрофа, глобальное разделение и экономические проблемы.

Технологии – ключ к решению основных проблем, стоящих перед человечеством в 21 веке. Тем не менее, недавние явления показывают, что технологии могут нанести ущерб сотрудничеству и даже ускорить глобальный конфликт: опасения по поводу автономного оружия, биотехнологий, государственного надзора и дезинформации теперь занимают центральное место в дискурсе вокруг цифрового управления[655]. Государственные и негосударственные субъекты, политики должны понимать, как глобальный Интернет фрагментируется, чтобы предвидеть и устранять ключевые источники потенциальных конфликтов. Одним из аспектов этого понимания является

---

[654] «Противостояние кризису глобального управления». Отчет Комиссии по глобальной безопасности, (2015).
[655] Анупам Чандер и Юен П. Ле. «Национализм данных». Юридический журнал Эмори, Vol. 64 (2015), стр. 677-739.

ответ на вопрос, как и почему страны расходятся в подходах к управлению данными. Отсутствие последовательной основы для анализа этих различных подходов препятствует гармонизации национальных интересов и препятствует усилиям международных организаций по созданию четких обязательств в отношении возникающих технологических проблем, таких как искусственный интеллект, цифровое наблюдение и трансграничные потоки данных.

Чтобы обратиться к концептуальной проблеме цифровой фрагментации, в этой статье вводится новый термин – режим данных. Режим данных относится к уникальному сочетанию управленческого потенциала, экономической политики и поведенческих практик, которые конкретизируют познаваемую позицию в отношении управления данными. Мы определяем типологию режимов данных с помощью набора руководящих критериев, которые помогают классифицировать различные варианты того, как правительства регулируют данные. В этой статье не делаются какие-либо нормативные суждения о режимах данных, но она направлена на то, чтобы описать, как заинтересованность правительства в усилении контроля в фрагментированном мире кристаллизируется в конкретные стратегии управления данными. Кроме того, описанная ниже структура не дает конкретного ответа на вопрос о том, как государства могут гармонизировать свои режимы данных. Скорее, он служит всеобъемлющей концептуальной линзой, через которую государства могут не только рационализировать создание норм в цифровой сфере, но и понять возможные расхождения в этой сфере в ближайшем будущем.

Наконец, эта концепция возникла в ответ на очевидный пробел в недавней литературе по темам, касающимся конфиденциальности данных, искусственного интеллекта и цифровой политики. Несмотря на то, что существует множество структур, регулирующих обсуждение роли правительства в технологии (и роли технологий в правительстве), многие из этих структур имеют дело с конкретными и узкими темами, не обращая внимания на то, как эти проблемы связаны с гораздо более крупными процессами и явлениями в настоящее время перед миром сегодня[656]. Безусловно, эти рамки служат полезными инструментами для выявления важных проблем, связанных с пересечением технологий и правительства, и, следовательно, формируют решающую основу для дальнейших исследований по этому вопросу. Концепция режимов данных основывается на этих моделях, чтобы еще больше затенять некоторые возникающие тенденции в следующем

---

[656] См., Например, «Государственный индекс готовности к искусственному интеллекту 2019 г.» Oxford Insights (2019), https://www.oxfordinsights.com/ai-readiness2019; Права человека в эпоху искусственного интеллекта, Access Now (2018); Марк Латонеро, «Управление искусственным интеллектом: защита прав человека», Data & Society (2018); Эйлин Донахью и Меган МакДаффи Мецгер, «Искусственный интеллект и права человека», журнал демократии, Vol. 30, № 2 (2019); Белая книга «Как предотвратить дискриминационные результаты в машинном обучении», Всемирный экономический форум (2018 г.); Сэм Сакс и Джастин Шерман, «Глобальное управление данными: концепции, препятствия и перспективы», Новая Америка (2019).

десятилетии. Авторы надеются, что такая линза будет полезна для политиков, частного сектора и других заинтересованных сторон для преодоления разногласий, предотвращения широкомасштабного ущерба и значимого вовлечения международных субъектов.

Режим данных: определение и критерии

В целом режимы данных формируют основу, с помощью которой страны регулируют Интернет и используют цифровые технологии для достижения заявленных и неустановленных целей[657]. Государства могут регулировать цифровое пространство с помощью различных инструментов, включая экономическую политику, законодательство о конфиденциальности, рыночный и инфраструктурный контроль, а также военные мощность. Режимы данных также отражают нормативные ценности, которые государства приписывают своим интересам в цифровой сфере. Страны могут использовать эти инструменты различными способами и по ряду причин, учитывая сложность пересекающихся интересов.

Режимы данных охватывают больше, чем модели управления данными или подходы к управлению данными. Последние концепции часто относятся к конкретному политическому выбору, который правительства делают в отношении трансграничных потоков данных и конфиденциальности информации[658]. Таким образом, эти термины, как правило, подчеркивают, как правительства регулируют сбор и использование данных частным сектором или передачу данных за пределы страны.[659] Режимы данных идут дальше, охватывая более широкие стратегические цели, которые правительства принимают для активного определения и создания параметров цифрового пространства и основных ценностей или норм, которые управляют Интернетом на международном уровне. Действительно, режимы данных лежат в основе того, как государства отстаивают свои стратегические интересы в Интернете и изменяют объем своего суверенитета в цифровую эпоху. Наконец, хотя режимы данных включают модели управления данными, они также содержат геополитический компонент, который выходит за рамки влияния на поведение частного сектора. Как обсуждается ниже, режимы данных дополнительно показывают, как государства активно формируют рынок, и возможность

---

[657] Заявленные цели являются официальными причинами, такими как экономический рост, создание рабочих мест или национальная безопасность. Неустановленные цели - это те, которые лежат в основе более крупных исторических тенденций, таких как торговый рычаг, ответные меры и контроль.

[658] Барбара Л. Кон, «Управление данными: императив качества в эпоху больших данных, открытых данных и за ее пределами». Журнал права и политики для информационного общества (2014).

[659] См. Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground (2015).

многостороннего взаимодействия и создания коалиций в цифровом пространстве.

В этой статье предлагаются следующие критерии, позволяющие разобраться в различиях в режимах данных и лучше понять, как различные инструменты и причины, лежащие в основе технологической политики, совпадают последовательным и предсказуемым образом. Каждый критерий представляет собой центральную ось режима данных государства и включает в себя конкретную политику и их обоснования. Авторы выбрали эти критерии на основе широких политических дискуссий, которые они получают, их важности для экономического роста и важности расширения цифрового влияния, которое они предлагают. Кроме того, в этом документе собраны эти критерии, чтобы восполнить предполагаемые пробелы в других типологиях управления данными, одновременно подтверждая основные идеи, уже сделанные в появляющейся литературе по данным и политике.

Критерий 1 – Трансграничные потоки данных и локализация

В настоящее время цифровизация затрагивает все аспекты экономической деятельности и становится все более важной в повседневной жизни.[660] Этот процесс создал совершенно новую экономику, сосредоточенную вокруг информации: такие отрасли, как облачные вычисления, аналитика больших данных и электронная коммерция, теперь вносят значительный вклад в ВВП.[661] Он также изменил производственный процесс и сыграл ключевую роль в реконфигурации глобальных цепочек поставок после структурных преобразований 1970-х.[662]

[660] Под цифровизацией мы понимаем процесс автоматизации и координации задач с помощью информационно-коммуникационных технологий (ИКТ).

[661] «Измерение цифровой трансформации: дорожная карта на будущее». ОЭСР (2019), стр. 20.

[662] Скотт Лэш и Джон Урри. Конец организованного капитализма. (1987), стр. 196-209. Джеффри Хендерсон. Глобализация высокотехнологичного производства. (1989).

Цифровая революция привела к беспрецедентному увеличению трансграничного потока данных.

Оценки показывают, что за последние 10 лет глобальные потоки данных увеличили мировой ВВП примерно на 10%, при этом объем глобальной пропускной способности вырос в 148 раз за тот же период.[663] Трансграничные потоки данных включают данные, сопровождающие международную торговлю, компьютеры и информацию услуги и обмен данными внутри корпораций.[664] Этот ошеломляющий объем передачи данных привел к ряду попыток правительства отрегулировать то, что в настоящее время является важнейшим компонентом экономической деятельности и торговли.

Чтобы отразить это, первый критерий вращается вокруг регулирования передачи данных между странами и обоснования политики. Ограничения на трансграничные потоки данных принимают несколько форм. Вообще говоря, это включает (i) категорический запрет на передачу данных за границу («Жесткая локализация»); (ii) требования к компаниям хранить копии данных на локальных серверах («Мягкая локализация»); (iii) требования к компаниям получить согласие или выполнить определенные условия перед передачей («Условные ограничения»)[665].

Источник: Фонд информационных технологий и инноваций (ITIF).

В некоторых отчетах подчеркивается раздвоенный подход к регулированию данных, основанный на моделях международной торговли[666]. На одном конце спектра находятся страны, которые склонны поддерживать либерализованный торговый режим; с другой – те, которые считают эти принципы вредными по ряду причин, не в последнюю очередь из-за асимметричного воздействия либерализации торговли на отечественные отрасли в неблагополучных странах[667]. Либеральная/протекционистская

---

[663] «Глобализация в переходный период: будущее торговли и цепочек создания стоимости». Глобальный институт McKinsey. (2019), стр. 14.

[664] «Цифровая глобализация: новая эра глобальных потоков». Институт McKinsey. (2016).

[665] Граница между этими политиками часто размыта, поскольку страны принимают комбинации мер локализации. Видеть. Мельцер, Дж. Лавлок, П. «Регулирование цифровой экономики: понимание важности трансграничных потоков данных в Азии. Институт Брукингса. (2018), стр. 5.

[666] 14 См., Например, Нир Хсетри, «Успех массовых онлайн-технологий в сборе средств: институциональная перспектива». Журнал международного менеджмента, Vol. 21, № 2. (2015), стр. 100–116. Дэни Родрик. «Политическая экономия торговой политики». Справочник по международной экономике. (1995), стр. 1457-1494; Шамель Азме и Кристофер Фостер. «TPP и повестка дня цифровой торговли». Международное развитие, № 16-175. (2016).

[667] «Либерализация» здесь означает торговые принципы, реализуемые через ГАТТ и торговый режим ВТО, такие как недискриминация, скоординированная предсказуемость и общее снижение торговых барьеров, таких

типология помогает объяснить основные причины, лежащие в основе ограничений потока данных. Предлагаем пять основных причин:

- Защита частной жизни граждан
- Государственный контроль над данными в правоохранительных целях
- Национальная безопасность, такая как предотвращение иностранного наблюдения
- Повышение экономической конкурентоспособности через «цифровое импортозамещение»

Взаимодействие с более развитыми странами с цифровой экономикой[668]

На практике эти доводы часто пересекаются множеством способов.[669] Каждое из этих обоснований занимает определенную точку в протекционистском спектре и отражает определенные цели политики, которые определяют режим данных.[670]

Критерий 2 - Рамки защиты персональных данных и конфиденциальности

Наш второй критерий касается того, как правительства взаимодействуют с растущим осознанием социальных проблем, связанных с цифровой экономикой.[671] Одновременно с цифровой революцией распространение личных данных через базы данных, сети связи и устройства для генерации данных привело к глубоким преобразованиям в отношения между гражданами и правительствами.[672] Огромный объем данных, генерируемых сегодня –

как тарифы и квоты. Джагдиш Бхагвати, Правин Кришна и Арвинд Панагария. «Мировая торговая система: тенденции и вызовы». Представлено на Конференции по торговле и флагу: изменение баланса сил в многосторонней торговой системе. (2014).

[668] Мельцер, Дж. Лавлок, П. «Регулирование цифровой экономики: понимание важности трансграничных потоков данных в Азии. Институт Брукингса. (2018), стр. 5.

[669] «Локализация данных: вызов глобальной торговле и свободному потоку информации». Группа Олбрайт Стоунбридж (2015), стр. 12-15.

[670] В данной статье не содержится нормативной позиции относительно ценности этих законов или основных политических режимов государств, которые их принимают.

[671] Эти социальные проблемы многогранны, многогранны и занимают центральное место в традиционных теориях участия государства и демократического участия. Вводное резюме см. Кэрол Пейтман. Участие и теория демократии. (1970), стр. 40-53. Для более полного лечения см. Йозеф Шумпетер. Капитализм, социализм и демократия (1943); Юрген Хабермас. Кризис легитимации (1973); Гарри Экштейн. Разделение и сплоченность в демократии (1966); Роберт А. Даль. Кто правит? (1961); Г. Уильям Домхофф. Кто правит Америкой? (1967); ТН Маршалл. «Гражданство и социальный класс» Серия лекций Кембриджского университета (1949).

[672] Даниэль Троттье и Кристейн Фукс. «Теоретические основы социальных сетей, политики и государства». Социальные сети, политика и государство: протесты, революции, беспорядки, преступность и полицейская

оцениваемый в 10,6 зеттабайт – намного превосходит уровни, измеренные даже десять лет назад, что способствовало появлению сложной экосистемы данных и рынка, прогнозируемого на уровне 49 миллиардов долларов.[673]

В ответ на эти изменения политики начали вводить юридические требования в отношении коллекции, обработка и использование личной информации[674]. Это множество инструментов политики, включая законы, постановления, отраслевые стандарты, правительственные инициативы и международные соглашения, составляет важную основу для управления данными в государственном секторе.[675] Хотя всесторонний анализ этих законов выходит за рамки этого документа распространение рамок конфиденциальности в государственном и частном секторах стало ключевым звеном в разработке политики и организационном управлении и варьировалось в зависимости от национального контекста[676].

Это расхождение привело к растущей фрагментации режимов данных и правовой архитектуры, лежащей в их основе.[677] Обоснование введения ограничений на то, как частные и государственные субъекты используют личные данные, имеет решающее значение для понимания этой фрагментации. На одной стороне спектра находятся страны, которые разрабатывают законы о конфиденциальности для экономических целей (например, для защиты

деятельность в эпоху Facebook, Twitter и Youtube. (2014).

[673] Шанхонг Лю, «Большие данные, статистика и факты», Statista (2019). https://www.statista.com/topics/1464/big-data/; Томас А. Сингхерст и др., «Электронная конфиденциальность и защита данных» CitiGroup.

[674] Требования к защите данных включены в положения о трансграничных данных, таких как действующий Соглашение о защите конфиденциальности между ЕС и США. Но хотя в большинстве стран существуют определенные меры защиты данных, степень и объем этих ограничений различаются. Кроме того, заявленные доводы в пользу этих положений также противоречивы, что приводит к еще большей фрагментации усилий стран по согласованию программ цифровой торговли друг друга. Например, одна неудача в продолжающемся процессе переговоров по Региональному комплексному экономическому плану (RCEP) связана с разногласиями по поводу надлежащей структуры защиты данных для трансграничной передачи данных. В то время как Япония твердо привержена либерализации потоков данных в соответствии со своим Законом о защите личной информации (APPI), некоторые страны, такие как Малайзия и Таиланд, выразили свою обеспокоенность по поводу такого типа правового воздействия. Кроме того, аналогичные проблемы существуют для гармонизации Рамок конфиденциальности Азиатско-Тихоокеанского экономического сотрудничества (АТЭС) с Рамками АСЕАН по управлению цифровыми данными и установления последовательного режима соблюдения конфиденциальности. См. В целом Тио Цзе Гана «Защита данных и конфиденциальности в АСЕАН - что это означает для бизнеса в регионе?» Deloitte. (2018); Акеми Сузуки и Томохиро Секигучи, «Защита данных и конфиденциальность» Нагашима Оно и Цунемацу. (2019). https://gettingthedealthrough.com/area/52/jurisдикция/36/data-protection-privacy-japan/; Кенсаку Такасе, «Соответствие GDPR: Закон Японии о защите личной информации». IAPP (2017). https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/;

[675] ключевые рамки

[676] Многие ключевые рамки конфиденциальности произошли от справедливой информационной практики Организации экономического сотрудничества и развития (ОЭСР). Директива ЕС 1995 года и последующий Регламент Общего регламента по защите данных (GDPR) во многом совпадают с принципами, а также с Законом Калифорнии о конфиденциальности потребителей (CCPA) 2018 года. Роберт Геллман. «Честная информационная практика: базовая история». CCPH (2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

[677] «Ключи к защите данных». Privacy International. (2018); Шон Макдональд и Сяо Мина, Внешняя политика «Истерзанная войной сеть». (19 декабря 2018 г.). https://foreignpolicy.com/2018/12/19/the-war-torn-web-internet-warring-states-cyber-espionage/#map

потребителей) или из соображений политического выбора (например, для контроля государственного сектора над цифровой экономикой)[678]. Эти законы и постановления часто ставят кибербезопасность выше личной конфиденциальности и отражают цели укрепления интересов безопасности от кибершпионажа или иностранного вмешательства в инфраструктуру связи.[679] С другой стороны, это модели управления, которые, как правило, защищают конфиденциальность как фундаментальное право человека[680]. Эти модели, как правило, подчеркивают вредные социальные последствия новых технологий, такие как алгоритмическая предвзятость и дискриминация, повсеместное наблюдение и потеря работы.[681] Мы признаем, что на практике страны часто колеблются между этими двумя концептуальными обоснованиями.[682]

Критерий 3 - Цифровая промышленная политика

Под цифровой промышленной политикой понимается попытка государства создать благоприятную среду для технологического развития путем распределения ресурсов, чтобы помочь отраслям, которые вращаются вокруг данных.[683] Промышленная политика вокруг ИИ и Интернета стала

---

[678] Например, Закон о разъяснении законного использования данных за рубежом (CLOUD) в США был принят в 2018 году как прямой результат решения Microsoft, ограничивающего право правоохранительных органов принуждать цифровые компании к общению между отдельными лицами. Видеть. Стивен П. Маллиган. «Трансграничный обмен данными в соответствии с Законом об облаках». R45173 Исследовательская служба Конгресса. (2018). В Китае Закон о кибербезопасности (CSL) направлен на обеспечение того, чтобы цифровые и телекоммуникационные компании, работающие в пределах китайской юрисдикции и обрабатывающие личные данные китайских граждан, не вмешивались в национальную экономическую политику. Видеть. «Режим защиты данных в Китае». Генеральный директорат Европейского парламента по международной политике. (2015).

[679] См., Например, Основной закон о кибербезопасности в Японии (2014 г.), Закон Китая о кибербезопасности (2016 г.), Закон о кибербезопасности в Сингапуре (2018 г.), Закон о кибербезопасности во Вьетнаме (2018 г.).

[680] Эта традиция частично вытекает из ключевых международных соглашений по правам человека. Например, статья 12 Всеобщей декларации прав человека (ВДПЧ) содержит часто цитируемую ссылку на защиту частной жизни, которая повлияла на другие важные договоры, такие как Международный пакт о гражданских и политических правах (МПГПП) и Конвенция о правах человека. Ребенок (CRC). Другими примерами этого являются Резолюция Генеральной Ассамблеи ООН о праве на неприкосновенность частной жизни в эпоху цифровых технологий от 2016 г. 71/199, Европейская конвенция о защите частных лиц в отношении автоматической обработки персональных данных (Конвенция 108) и Арабская хартия прав человека. Видеть. «Международные стандарты конфиденциальности». Фонд электронных рубежей. (2018). https://www.eff.org/issues/international-privacy-standards

[681] «Ключи к защите данных». Privacy International. (2018); «Права человека в эпоху искусственного интеллекта». Доступ сейчас (2018).

[682] Например, Мексика закрепила защиту конфиденциальности в своей Конституции и приняла несколько федеральных законов о конфиденциальности, таких как Общий закон о защите личных данных государственными учреждениями, в основном для соблюдения требований ЕС в отношении коммерческого взаимодействия. «Государство конфиденциальности в Мексике». Privacy International (26 января 2019 г.). https://privacyinternational.org/state-privacy/1006/state-privacy-mexico

[683] Вместо того, чтобы рассматривать ИИ как «всеобъемлющий» революционный термин, который подразумевает все возникающие проблемы с технологиями, в данной статье используется узкое определение, ограничивающееся расширением технологий обработки данных и различными национальными политиками, которые их подчеркивают. Хорошее резюме дискуссии о промышленной политике см. Кристофер Фостер

одним из механизмов, с помощью которого правительства активно строят свое собственное видение цифрового пространства [684]. Эта политика принимает разные формы, включая: субсидирование (как прямое, так и косвенное), инновационные парки, налоговые и денежно-кредитные стимулы, долгосрочное стратегическое планирование, налоги на цифровые услуги, структурирование приобретения, лицензионные соглашения и прямые иностранные инвестиции.

Асимметричная структура глобальных цепочек создания стоимости (ГЦС) привела к разногласиям в том[685], как страны реализуют свои национальные цифровые стратегии[686]. Страны, которые изначально доминировали в области цифровизации, обычно преследуют стратегии, которые будут способствовать расширению своего цифрового производства на другие рынки, не позволяя конкурентам оспаривать их доминирование.[687] Напротив, страны, «догоняющие», могут проводить как защитную политику, ограничивающую проникновение глобальных информационных компаний на их внутренние рынки, так и агрессивную политику, которая стимулирует развитие их собственных технологических возможностей и структурных позиций[688].

Национальная политика может занять примирительную, конкурентную или изоляционистскую позицию по отношению к предполагаемой угрозе со стороны других цифровых компаний. С помощью примирительного взаимодействия страны согласовывают стратегии развития в соответствии с ранее существовавшими нормами и обычаями, чтобы сотрудничать с цифровыми транснациональными корпорациями для предполагаемой взаимной выгоды.[689] В отличие от этого, это конкурентный вариант, при котором страны

и Шамел Азме. «Новые экономики и национальная цифровая политика: перспектива промышленной политики». Журнал исследований развития (2019).

[684] Некоторые утверждают, например, что российский «Суверенный закон об Интернете» действует, чтобы установить больший контроль над Интернетом путем маршрутизации трафика через контролируемую государством инфраструктуру. Видеть. Алена Епифанова. «Расшифровка российского« суверенного закона об Интернете»» №2. Германский совет по международным отношениям (2020). https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

[685] Кристофер Фостер и Шамел Азме. «Новые экономики и национальная цифровая политика: перспектива промышленной политики». Журнал исследований развития (2019).

[686] Шон Макдональд и Сяо Мина, «Разорванная войной сеть» Внешняя политика. (2018).

[687] Хороший обзор этого в промышленном контексте см. Ха-Джун Чанг, Взбивая по лестнице: стратегия развития в исторической перспективе (2003); Санджая Лалл, «Технологические возможности и индустриализация». Мировое развитие (1992); Иммануал Валлерстайн Современная мировая система. (1974); Джованни Арриги. Долгий двадцатый век (1994); Ник Срничек, Платформенный капитализм (2016).

[688] Например, Национальная программа Индии по искусственному интеллекту предлагает использовать свой большой кадровый резерв для создания сквозных проектов, сосредоточив при этом больше внутренних ресурсов на развитии ключевых отраслей с интенсивным использованием данных внутри страны. Кроме того, предложенный в Индии закон о локализации данных, возможно, увеличил бы транзакционные издержки для иностранных фирм, тем самым изменив предпочтительность определенных услуг в стране. Видеть. «Национальная стратегия искусственного интеллекта #AIForAll». Нити Аайог. (2018); Ариндраджит Басу и др. «Гамбит локализации» Центр Интернета и общества, Индия. (2019); «Раскрытие потенциала экономики данных Индии. Омидьяр Сеть Индия. (2019).

[689] Правительство Зимбабве подписало соглашение об обмене данными со стартапом CloudWalk Technology из Гуанчжоу в 2018 году для развития инфраструктуры умного города, что было воспринято как взаимовыгодное

развивают свой собственный цифровой потенциал, а затем агрессивно конкурируют с другими транснациональными корпорациями в экспорте. товары и услуги для приобретения доли рынка за рубежом[690]. Наконец, страны могут выбрать изоляционистский путь, то есть выделение ресурсов для развития самодостаточности в наукоемких отраслях или расширение юридического суверенитета над цифровой территорией[691]. Структура признает, что на практике, страны принимают комбинации этих политических позиций[692].

Критерий 4 - Исследования и разработки в области искусственного интеллекта (НИОКР)

Этот критерий учитывает финансирование ИИ частным сектором, а также академические исследования и кадровый резерв глобального ландшафта ИИ. Огромный объем литературы по ИИ растет значительными темпами.[693] Действительно, согласно одной цифре, глобальный объем рецензируемых статей по ИИ увеличился на 300% с 1998 по 2018 год.[694] Вместе с этим произошел резкий рост венчурного капитала ИИ. финансирование и участие государственного сектора в стимулировании развития новых технологий[695]. В 2019 году глобальные частные инвестиции в ИИ составили более 70 миллиардов долларов, из которых (37 миллиардов долларов) пошли на стартапы, а другая (34 миллиарда долларов) пошла на слияния и поглощения

соглашение. Линси Чутел. «Китай экспортирует программное обеспечение для распознавания лиц в Африку, расширяя свою обширную базу данных». Кварц Африка. (25 мая 2018 г.). https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

[690] Китай занимает эту позицию по отношению к США и их глобальным цифровым компаниям. В то время как этот документ отказывается войти в дискуссию, он признает роль промышленной политики Китая в стимулировании своих собственных возможностей высокотехнологичные и теперь перспективные планы развития (например, пояса и дорожной Initiative (带–路), Сделано в Китае к 2025 году). Видеть. Джеффри Динг. «Расшифровка китайской мечты об ИИ». Институт будущего человечества. (2018); Мартина Ф. Ферракане и Хосук Ли-Макияма. «Технологический протекционизм Китая и его необъяснимые основания. Европейский центр международной политической экономии. (2016).

[691] На самом деле, первое маловероятно с учетом порогового уровня затрат на основной капитал для развития высоких технологий, но может материально проявиться в определенных контекстах. Например, недавняя технологическая траектория Кубы иллюстрирует эту возможность. Энн Нельсон. « Параллельные миры Кубы: цифровые медиа преодолевают пропасть». Центр содействия международным СМИ. (2016), стр. 13.

[692] Например, Кения в разные моменты принимала все три в зависимости от контекста и вовлеченного партнера по переговорам. Каришма Банга и Дирк Виллем те Велде. «Как развивать производство и создавать рабочие места в цифровой экономике: 10 приоритетов политики для Кении. « Поддержка экономических преобразований» (2018), стр. 7-13.

[693] См. Грейс Кисер и Йоан Манта. «Global AI Talent Report 2019». Jfgagne. (2019). https://jfgagne.ai/talent-2019/

[694] «Отчет об индексе искусственного интеллекта за 2019 год». Стэнфордский институт искусственного интеллекта, ориентированного на человека (2019), стр. 5.

[695] Глобальное исследование инициатив частного сектора см. Майкл Чуй и др. «Записки с границы искусственного интеллекта» Глобальный институт McKinsey. (2018). Для разбивки инициатив государственного сектора см. Тим Даттон, «Обзор национальных стратегий ИИ». Средний (2018). «Составление карты нормативных предложений для искусственного интеллекта в Европе». Доступ сейчас (2018).

(«M&A»)[696].

Таким образом, объем ресурсов, выделяемых странами и странами на развитие ИИ, указывает на их возможности и намерения проецировать власть. Хотя есть разногласия по поводу того, какие страны инвестировали больше и «возглавляют» развитие ИИ, мы отказываемся вдаваться в эту дискуссию.[697] Вместо этого, эта структура в основном фокусируется на степени, в которой государства инвестировали и привлекали человеческий и физический капитал для поддержания своей репутации в области ИИ. По сравнению с цифровой промышленной политикой этот критерий отражает чисто экономическую и инвестиционную мощь, а не какой-либо конкретный набор вариантов политики. Например, в стране может быть мало возможностей ИИ, но, тем не менее, она предлагает надежную национальную стратегию по причинам репутации – этот критерий служит для учета этого аспекта и дальнейшего уточнения фактических темпов привлечения талантов и прямых иностранных инвестиций («ПИИ»).

Более того, образовательный потенциал для работы в глобальном инновационном пространстве также подразумевает способность правительств анализировать и каталогизировать общедоступные статистические данные, такие как данные переписи населения или здоровье и поведение потребителей. Государства, отстающие в этом статистическом потенциале, часто сталкиваются с трудностями при включении аналитики данных в цепочки создания стоимости и сталкиваются с ограничениями при разработке технологических решений для частного сектора. Без общедоступных данных предприятия не имеют доступа к ключевым ресурсам, которые они используют для разработки, тестирования и внедрения своих услуг, что препятствует реализации более широкой государственной стратегии обработки данных и усиливает отсутствие у страны ноу-хау или инвестиций в высокие технологии.[698] наносят вред образовательным инициативам, создавая петли обратной связи: сокращение кадровых резервов усиливает административные пробелы и стимулирует стимулы к утечке мозгов из-за ограниченных

---

[696] «Отчет об индексе искусственного интеллекта за 2019 г.» Стэнфордский институт искусственного интеллекта, ориентированного на человека (2019), стр. 4-5.

[697] Редко когда какие-либо исследования отрицают, что на Китай и США приходится самая большая в мире доля НИОКР, связанных с ИИ. Споры в основном сосредоточены вокруг того, кто из этих двух действительно возглавляет следующую революцию цифровых технологий. Смотри в общем. Уильям А. Картер и Уильям Д. Крамплер. «Умные деньги на достижениях Китая в области искусственного интеллекта». Центр стратегических и международных исследований. (2019), стр. 13. Райан Хасс и Зак Балин. «Отношения США и Китая в эпоху искусственного интеллекта». Институт Брукингса. (2019). https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/

[698] Стив Макфили и Нур Барнат. «Создание статистического потенциала для устойчивого развития: разработка основ, необходимых для современных национальных статистических систем». Европейская экономическая комиссия Организации Объединенных Наций (2016), стр. 2-4.

возможностей дома.[699] Хотя сфера применения этой концепции в первую очередь сосредоточена на государствах и их институциональных субъектах, она, тем не менее, не игнорирует важность поведения частного сектора для управления данными.

Критерий 5 - Инфраструктура и развитие

Цифровая инфраструктура – это физические и сетевые системы, которые люди используют для передачи информации, услуг и цифровых битов. Это определение включает в себя как телекоммуникационную инфраструктуру, так и физическую инфраструктуру, которая содержит как информационные, так и цифровые компоненты («гибридная инфраструктура»)[700]. Тщательная типология цифрового управления должна включать анализ уровней развития цифровой инфраструктуры. С одной стороны, возможности сетевых коммуникаций помогают определить историческую последовательность участия страны в цифровой революции в прошлом.[701] Действительно, деятельность в онлайн-пространстве невозможна без некоторой формы сетевой емкости. С другой стороны, инфраструктура помогает определить текущее положение страны в отношении будущего цифрового развития. Действительно, способность страны проецировать силу для консолидации своих интересов в цифровом пространстве и влияния на создание норм зависит в первую очередь от ее способности участвовать в игре[702]. Более того, страны могут провозглашать свои инфраструктурные обязательства в тандеме с другими целями разработки политики, такими как сокращение цифрового разрыва, развитие умных городов будущего и подготовка кадров завтрашнего дня[703].

Как и в случае с другими показателями управления данными, в составном индексе развития инфраструктуры наблюдается значительное расхождение

---

[699] «Global Talent 2021: Как новая география талантов изменит стратегии управления человеческими ресурсами». Oxford Economics. (2020); «Глобальный риск талантов - семь ответов». Всемирный экономический форум (2011), стр. 9.

[700] Айкут Атали, Чандра Гнанасамбандам и Бхаргс Шриватсан. «Преобразование операций инфраструктуры для мира гибридного облака. McKinsey & Company (2019). https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/transforming-infrastructure-operations-for-a-hybrid-cloud-world#

[701] Том Форестер. Революция информационных технологий, (1980); Мелвин Кранцберг. «Информационный век: эволюция или революция?» Информационные технологии и социальная трансформация, (1985).

[702] Роберт Д. Аткинсон. «Руководство по цифровой инфраструктуре для политиков». Фонд информационных технологий и инноваций. (2016), стр. 3-5.

[703] Дурбан, Южная Африка, является одним из примеров, когда муниципальные власти с помощью государства могут использовать интеллектуальные технологии для стимулирования инновационного и устойчивого роста и привлечения внимания других стран к этому процессу. Ключевым компонентом трансформации Дурбана, в результате которого город был выбран Фондом Рокфеллера в качестве пионера программы «Устойчивые города», была возможность связать управление инфраструктурой с аналитикой данных. «Глобальные уроки из проблем Дурбана, связанных с изменением климата». Новый гуманитарный. (24 мая 2011 г.). http://www.thenewhumanitar.org/news/2011/05/24/global-lessons-durban-s-climate-change-challenges

между странами, заявившими о доминирующем положении в глобальной цифровой экономике, и странами, которые опоздали к этому процессу.[704] Но в отличие от других источников цифровой власти, телекоммуникационная инфраструктура не является полностью диспозитивной с точки зрения геополитического контроля над цифровым пространством[705]. Страна или регион могут иметь сильное развертывание широкополосной связи, но не иметь других возможностей (например, привлечения талантов, финансирования).

Скорее, сетевая инфраструктура[706] является важной основой, через которую все страны реализуют свои интересы в области цифрового управления. Этот критерий признает важность 5G и Интернета вещей (IoT) для понимания недавней фрагментации цифрового управления и борьбы за цифровую территорию.[707] Предыдущие достижения в области беспроводной связи привели к тому, что несколько государственных субъектов заявили о лидерстве в развертывании аппаратного оборудования и создании спецификаций. и технические стандарты, поддерживающие совместимость цифровых технологий.[708] Отличие 5G заключается как раз в нынешнем процессе фрагментации, который превратил инновации в области данных в столь спорную сферу геополитической и экономической конкуренции. В сочетании с растущим значением IoT для повседневных экономических транзакций сетевая инфраструктура помогает оценить будущие цифровые перспективы страны и ее положение на более широкой конкурентной арене[709].

---

[704] «Глобальное исследование электросвязи 2019», Ernst & Young (2019), стр. 4.

[705] Конкуренция между США и Китаем в области 5G показывает, что, хотя пропускная способность сети является ключевым показателем мощности, она сама по себе не может определять лидерство в цифровом пространстве. Хотя многие подчеркивали связь между распространением Huawei и способностью китайцев влиять на установление стандартов, никто не мог сомневаться в том, что крупные технологические компании США возглавили цифровую революцию и будут продолжать занимать центральное место в ее продолжающемся процессе.

[706] Европа является ярким примером такой ситуации. Видеть. Ник Уоллес и Даниэль Кастро. «Влияние нового постановления ЕС о защите данных на ИИ». Центр инноваций в области данных. (2018), стр. 2-4; Джон Х. Честнат. «Развертывание широкополосной связи в США и в Европе: что говорят данные?» Центр технологий, инноваций и конкуренции. (2014).

[707] 5G относится к следующему поколению беспроводной связи, в котором будет наблюдаться беспрецедентный рост объема потоков данных и сетевых подключений. IoT относится к распространению интеллектуальных устройств, соединяющих цифровой и физический миры, и к процессу, который в дальнейшем будет способствовать созданию сложной экономики, основанной на данных.

[708] Лидерство в инновациях в области беспроводной связи является предметом горячих споров, поскольку статус «первопроходца» обычно дает компаниям преимущество в раннем приобретении доли рынка за счет «сетевого эффекта». Кэтрин Такер. «Сетевые эффекты и рыночная власть: чему мы научились за последнее десятилетие?» Антимонопольное право (2018). http://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf.

[709] Стокгольм, Швеция - один из ярких примеров того, как цифровая инфраструктура влияет на стратегии устойчивого развития. Гидроэнергетика и мощные электрические сети составляют основу руководства страны в отношении устойчивого проектирования городов. Для сравнения, Торонто, Канада, также может похвастаться внедрением технологий умного города.

Критерий 6 - Административный потенциал и регулирование

Административный потенциал в стране отражает не только степень, в которой государства могут применять механизмы управления данными, но и структурные отношения между частным и государственным секторами. Хотя точное определение этого термина горячо оспаривается, авторы подходят к нему с учетом двух основных концептуальных оснований. Во-первых, административный потенциал отражает функциональный аспект в смысле государственного управления: это способность сложной бюрократии выполнять действия с помощью правовых инструментов от местного до национального уровня[710]. Кроме того, в этом документе также признается, что этот термин содержит компонент власти, то есть способность государства насильственно применять политические решения, регулируют социальные отношения, распределяют ресурсы определенным образом и мобилизуют сотрудничество для достижения целей.[711]

Поскольку в данной статье этот термин используется таким описательным образом, в нем отказывается рассматривать роль коррупции или тип правительства для анализа режимов данных. Исследования, которые сосредоточены исключительно на правительственной структуре, как правило, предполагают, что правильные стандарты управления данными связаны с определенными правительственными режимами или существующими международными нормами[712]. Тем не менее, авторы признают, что во многих обстоятельствах эти показатели действительно объясняют сложное поведение и служат полезными инструменты для выявления ограничений в реализации политики, эффективном управлении и прозрачности.

После этого административный потенциал помогает измерить возможность соблюдения законов и, следовательно, выступает в качестве еще одного критерия для анализа управления данными. Существование и распространение законов, нормативных актов и политических целей в отношении цифровых инноваций и киберпространства было бы незначительным, если бы государство не могло фактически реализовать их и

---

[710] Питер Дж. Мэй. «Разработка и реализация политики». Справочник по государственному управлению (2003 г.); Берил. А. Радин. «Инструменты межгосударственного управления». Справочник по государственному управлению (2003 г.). Питер Морган. «Развитие потенциала: введение». Новые проблемы в развитии потенциала: материалы семинара. (1993).

[711] Майкл Манн разбивает это понятие на два компонента: «деспотическая» и «инфраструктурная» власть. Майкл Манн. Источники социальной власти (1986). Для обработки работы Манна см. Джоэл С. Мигдал. Государство в обществе, (2012).

[712] Сьюзан Ааронсон, «Поворот к торговым соглашениям для регулирования Интернета», в работе Жан-Батиз Велют и др., В книге «Понимание соглашений о мега-свободной торговле: политическое и экономическое управление нового межрегионального взаимодействия» (2017); Стивен Фельдштейн. «Глобальное расширение слежки за ИИ». Фонд Карнеги за международный мир (2019).

повлиять на конкретное поведение. Действительно, многие страны приняли законы о защите данных, но им трудно обеспечить их соблюдение, не обеспечить их соблюдение из-за нехватки ресурсов и процедурных задержек.[713] Такая вариативность в правоприменении меняет поведение субъектов, которые либо (i) должны соблюдать законы данная страна; (ii) вести переговоры с данной страной на международном уровне; или (iii) принимать, применять или пересматривать законодательство самостоятельно.

Что касается первого случая, корпорации и другие субъекты хозяйствования должны скорректировать свои модели оценки рисков при использовании рыночных возможностей, чтобы сбалансировать затраты на соблюдение требований и неопределенность. Кроме того, репутация из-за отсутствия правовой защиты может нанести ущерб способности страны проецировать свою цифровую мощь за границу или влиять на создание норм. В частности, репутация, связанная с административным потенциалом, также включает способность государств использовать технологии для реагирования на кризисы или серьезные проблемы.[714] Такая репутация включает как предполагаемые, так и соответствующие компоненты: государства могут использовать технологический потенциал для решения ожидаемой проблемы или реагирования на существующую. . Эти соображения влияют на позицию, которую государство примет, чтобы преследовать свои собственные интересы.

Более того, административный потенциал также демонстрирует уникальный баланс интересов между государственными и частными заинтересованными сторонами в данной стране. Этот баланс интересов частично объясняет конкретное формирование политики, а также нормативный подход, применяемый государствами к цифровой сфере.[715] Таким образом, он охватывает различия в роли государства в экономике и подходы, используемые для изменения частного поведения. Некоторые государства заняли жесткую позицию в утверждении влияния на цифровую экономику[716].

---

[713] См. Указатель верховенства закона. World Justice Project, (2019).

[714] Важно отметить, что меры общественного здравоохранения, принятые правительствами в ответ на распространение Covid-19, демонстрируют эту способность. Страны Восточной Азии, такие как Китай и Южная Корея, использовали комплексную аналитику данных для прогнозирования распространения вируса и использовали свою инфраструктуру электронной коммерции для доставки товаров непосредственно инфицированным людям. Джастин Фендос. «Уроки вспышки COVID-19 в Южной Корее: хорошее, плохое и уродливое». Дипломат (10 марта 2020 г.). https://thediplomat.com/2020/03/lessons-from-south-koreas-covid-19-outbreak-the-good-bad-and-ugly/

[715] «Видение 2030» Саудовской Аравии содержит программу управления цифровыми инициативами, направленную на изменение экономической модели страны с помощью инновационных технологий и молодых талантов. Создание стратегии стало результатом признания лидерами Саудовской Аравии необходимости диверсифицировать экономический рост, не ограничиваясь добычей нефти, и изменить общую цифровую позицию страны в 21 веке. «Раскрытие потенциала цифровой экономики Королевства Саудовская Аравия». Эрнст энд Янг, (2019).

[716] Помимо США и Китая, некоторые другие примечательные примеры - Южная Корея, Индонезия и Вьетнам. Видеть. Ли Джункю. «Структура торговли Кореи и ее политические вызовы». Будущее корейской торговой политики, (2012 г.); Тереза Умали. «Развитие цифровой экосистемы Индонезии». OpenGov Asia (29 августа

Другие в разные моменты были менее активны в этом отношении и вместо этого сосредоточились на том, чтобы частный сектор возглавил процесс цифровизации.[717]

Критерий 7 - Лидерство и власть

Наконец, любая значимая классификация цифрового управления должна иметь некоторую оценку лидерства и власти. Как и административный потенциал, власть – сложный термин, который часто вызывает больше разногласий, чем консенсуса.[718] Мы называем власть способностью государства оказывать давление на другие государства, чтобы они уступали их интересам. Однако эта способность не всегда проста. Как обсуждается ниже, существует ряд инструментов, доступных государству для реализации своей власти, включая грубую силу (как военную, так и экономическую), определение повестки дня и создание глобальных норм.[719] Хотя каждый из этих инструментов может позволить государству оказывать давление на других – то, как они действуют, отражает заметные теоретические различия.

Грубая сила, возможно, самая простая, но самая агрессивная тактика, заходит так далеко только потому, что она действует в индивидуальном порядке и ее относительно легко потерять.[720] Сохранение способности грубой силы требует обеспечения того, чтобы все участники не могли эффективно бросить вызов доминирующей силе. Постановка повестки дня может возникнуть в результате грубой силы (т. Е. Негативной обусловленности), но также может быть получена независимо.[721] Поскольку установление повестки дня позволяет актеру исключить возможность реализации его интересов другим актором, эта форма власти является более сложной, чем грубая сила и идет дальше в своей работе[722]. Наконец, хотя установление повестки дня может

2019 г.). https://www.opengovasia.com/developing-indonesias-digital-ecosystem/ Prema-chandra Athukorala. «Реформы торговой политики и структура защиты во Вьетнаме». Мировая экономика, Vol. 29. № 2. (2006), стр. 161–187.

[717] Израиль является примером этого явления, которому не уделяют должного внимания. Его экономика созрела с инновационным потенциалом и с начала 2000-х годов стала рассадником цифровой деятельности, в которой сосредоточено большое количество стартапов, венчурных фондов и корпоративных центров НИОКР, причем без каких-либо протекционистских законов. Однако большинство этих стартапов сталкиваются с проблемами конкуренции с иностранными компаниями и обычно приобретаются более крупными игроками. Дэн Сеньор и Сол Сингер. Нация стартапов: история экономического чуда Израиля (2009 г.).

[718] Стивен МакНами и Майкл Глассер. «Концепция власти в социологии: теоретическая оценка». Гумбольдтский журнал социальных отношений, Vol. 15, No. 1. (1987), pp. 79-104.

[719] Обсуждение трансформации инструментов проецирования мощности за последние полвека см. У Мартина ван Кревельда. Трансформация войны (1991). Более философское изложение этой схемы власти см. У Стивена Льюкса. Власть: радикальный взгляд (1974).

[720] Там же, стр. 110–112.

[721] Маргарет Гроарк, «Власть, действие и структура», Новая политология, Том. 14, № 1 (1993).

[722] Адам Пржеворски, Капитализм и социал-демократия (1985).

изменить совокупность возможных вариантов, оно не меняет первоначального желания актера преследовать свой интерес. Создание глобальных норм, напротив, оказывает даже большее влияние, чем установление повестки дня, потому что оно не только определяет возможные варианты на столе, но и изменяет то, как государство определяет свои собственные интересы[723]. Поражает суть того, как другие участники определяют свои стратегические интересы. представляет собой невероятно мощный инструмент и представляет собой одну из высших форм власти, к которой может стремиться государство.

Эти три оси власти переплетаются с тем, как государства отстаивают свое влияние в Интернете, цифровом пространстве и будущем технологий через режимы данных. Они также создают иерархию лидерства в глобальном созвездии государств. Лидерство – важный компонент режимов обработки данных, потому что оно частично отражает то, как государства видят друг друга. Для этого критерия в статье предлагаются следующие измерения.

Во-первых, лидерство содержит репутационный компонент, который мы определяем как способность государства использовать свое предполагаемое положение власти для достижения целей своей политики и отстаивания своих интересов в цифровом пространстве[724]. Источником этой репутации является комплекс факторов, включая история, экономический потенциал, готовность к инновациям, нормотворчество, многостороннее и многостороннее участие и определение видения. Степень лидерства варьируется в зависимости от форума взаимодействия и лидерской позиции государств, участвующих во взаимодействии. Например, страна, не имеющая влияния по отношению к цифровому лидеру, может оказаться в более выгодном положении среди небольшой когорты[725].

Во-вторых, лидерство также включает в себя измерение, выходящее за рамки показателей мягкой силы.[726] Оно также включает военную жесткую силу и способность государства прибегать к угрозе силой или ее применению в исключительных обстоятельствах[727]. Авторы признают, что в то время как

---

[723] Стивен Льюкс. Власть: радикальный взгляд (1974).

[724] Авторы признают дискуссию в теории международных отношений об ограничениях определения того, что на самом деле «хочет» государство. Видеть. Александр Вендт. Социальная теория международной политики (1999). Тем не менее, мы предпочитаем согласиться с тем, что государства действительно действуют в своих собственных интересах и преследуют цели, основанные на этих интересах.

[725] Финляндия, Латвия и Эстония стали законодателями мод в борьбе с иностранным вмешательством в выборы и получили дипломатические и переговорные рычаги по этой теме по сравнению с другими государствами. Залив Себастьяна и Гуна Шноре. «Защита выборов: стратегический коммуникационный подход». Центр передового опыта стратегических коммуникаций НАТО, (2019), стр. 5.

[726] Термин «мягкая сила», означающий способность государства привлекать и влиять на другие государства посредством дипломатии, ассоциируется с Джозефом Найом. Мягкая сила: средства к успеху в мировой политике, (2004).

[727] Жесткая военная сила относится к агрессивному или оборонительному использованию экономических или военных средств для воздействия на поведение другого государства. Джозеф Най. Мягкая сила: средства к успеху в мировой политике, (2004). Для более широкого контекстуализации этой концепции по отношению к теории государства см. Макс Вебер, «Политика как призвание». Макс Вебер: Очерки социологии,

международно-правовые механизмы играют важную роль в формировании решений государства, связанных с кибервойной, многие из нынешних практик ведения кибервойны возникли через «серые зоны» в традиционных механизмах.[728] Эта сумеречная область международного права частично объясняет подход государства к управлению данными с точки зрения лидерства и власти, потому что он представляет собой неизведанные области, в которых создание прецедентов дает огромное преимущество тем, кто может сделать это успешно.

С геополитической точки зрения цифровое управление включает два измерения. С одной стороны, способность государства оказывать военную мощь через киберпространство извне в отношении других субъектов указывает на определенную степень власти. С другой стороны, способность государства использовать тактику цифровой полиции внутри страны в отношении своих собственных людей указывает не только на намерения государственного деятеля, но и на повсеместность его цифрового контроля. Хотя объединение определенных политических взглядов с внешними или внутренними методами цифрового контроля может дать интересные корреляции, само по себе это не дает полного понимания фрагментации глобального Интернета, потому что почти все страны к настоящему времени установили определенный уровень инфраструктуры наблюдения[729]. По этой причине наша типология не фокусируется на возможностях слежки как на независимом критерии оценки цифровой правительственной политики, а вместо этого предпочитает включать их в общий обзор военной мощи.

Прогнозы внешней мощи предполагают использование возможностей киберпространства для эксплуатации уязвимостей в ключевой коммуникационной, энергетической, финансовой, экономической и политической инфраструктуре целевой страны с целью оказания давления на лидеров посредством социальных потрясений.[730] Кибервозможности в наступательном смысле включают как использование компьютерных сетей («CNE»), компьютерных сетевых атак (« CNA ») и компьютерных сетевых атак («CND»).[731] Многие страны уже начинают инвестировать в массивные

переведенные Г. Х. Гертом и К. Райтом Миллсом (1946); Джорджио Агамбен, Homo Sacer (1995).

[728] Например, хотя Устав ООН может регулировать право государств прибегать к угрозе применения силы, многие нормы, существующие в отношении кибервойны, вышли за пределы черной буквы закона. Роберт Райнер. Политика полиции (2010 г.); Кубо Мачак. «Кризис международного права кибербезопасности?» 8-я Международная конференция по кибер-конфликтам, 2016 г., (2016), стр. 132-134.

[729] Шон Макдональд и Сяо Мина, «Разорванная войной сеть», Внешняя политика. (2018).

[730] Некоторые печально известные кибератаки включают: Yahoo! 2014 г. взлом, который скомпрометировал 200 миллионов идентификационных данных, утечка данных кредитной карты Equifax 2017 года, затронувшая 143 миллиона американских, канадских и британских клиентов, вирус Wannacry 2017 года и кибер-червь Stuxnet, нацеленный на иранский ядерный объект в Натанзе в 2010 году. «Коммодификация кибервозможностей: большой базар кибероружия». Программа государственно-частного аналитического обмена 2019. (2019), стр. 14-18.

[731] Подробное обсуждение этих терминов см. Росс М. Рустичи. «Кибероружие: выравнивание международного

оборонные ресурсы для развития стратегической готовности с целью сдерживания иностранных атак[732]. Запланированные оборонные соглашения между государствами иллюстрируют формирование рыхлой системы кибер-альянсов и могут указывать на будущие тенденции в международных отношениях[733].

Краткая типология

Этот раздел содержит краткую визуализацию рассмотренных выше критериев для описания типологической основы классификации режимов данных. Первые две критерии – трансграничные потоки данных и защита персональных данных – различают режимы данных в зависимости от характера политики. По этим двум критериям страны либо соответствуют квалификации, либо нет. Остальные критерии связаны с различиями в степени, то есть они измеряют положение, которое страна занимает в диапазоне от высокой до низкой емкости в зависимости от содержания критерия. Приведенная ниже таблица не является исчерпывающей и должна служить отправной точкой для дальнейшего анализа.

Таблица 1: Типологическая матрица режима данных

Вывод

По мере того как Интернет продолжает фрагментироваться и создавать пространство для формирования новых норм в цифровой сфере, правительства во всем мире начинают принимать множество политик, чтобы утвердить больший контроль над своими национальными судьбами и преследовать свои собственные интересы. Различия в практике управления данными между государствами и появление специальных режимов данных заслуживают

игрового поля». Параметры. (2011).

[732] Например, австралийская стратегия кибербезопасности 2016 года создала фонд в 230 миллионов австралийских долларов для повышения устойчивости инфраструктуры к кибератакам. Стратегия инициирует создание Австралийского центра кибербезопасности (ACSC), который координирует анализ разведывательных данных с другими австралийскими учреждениями, а также поддерживает ресурсы, предназначенные для финансовой и энергетической стабильности и безопасности выборов. Стюарт Фаулер и др. «Разработка политики кибербезопасности, которая распространяется на оборонные закупки Австралии». Журнал Сил обороны Австралии. (2017)

[733] Бенджамин М. Дженсен, Брэндон Валериано и Райан Мэнесс. Кибер-стратегия: развивающийся характер власти и принуждения. (2018).

особого внимания, поскольку будущие правила взаимодействия и цифрового контроля будут в значительной степени определяться современными тенденциями в киберпространстве. Чтобы лучше подготовить политиков к задаче минимизации вреда в глобальном конфликте данных, в этом документе была предложена концепция режимов данных или уникальное сочетание управленческого потенциала, экономической политики и поведенческих практик, которые конкретизируют познаваемую позицию в отношении управления данными. В частности, концепция режимов данных помогает устранить некоторые пробелы в других заметных типологиях возникающих проблем в управлении данными, искусственном интеллекте и цифровой экономике за счет включения геополитических и экономических расхождений в существующих подходах к регулированию данных. По сути, режимы данных поражают суть того, как государства активно создают и определяют масштабы цифрового пространства и Интернета. В документе изложены их основные критерии и будущие тенденции, которые могут проявиться в следующем десятилетии.

В документе изложены компоненты режимов данных, предлагая набор критериев для создания работоспособной основы для понимания растущей фрагментации цифрового пространства. Во-первых, политика, ограничивающая поток данных между странами, подчеркивает две важные особенности режимов данных: 1) способность государства напрямую контролировать цифровую торговлю; и 2) способность государства контролировать цифровые индустрии в пределах своих границ. Такая политика имеет множество причин, включая национальную безопасность и торговые рычаги. Одно из таких оснований – защита персональных данных – занимает особое место в режимах данных, поскольку затрагивает социальную проблему конфиденциальности и отражает то, как правительство воспринимает свои отношения со своим народом. Во-вторых, новые тенденции в цифровой промышленной политике также играют роль в глобальной фрагментации: страны могут реализовывать инициативы по лучшему оснащению своей национальной промышленности для цифрового будущего и тем самым создавать вредоносную конкуренцию с другими государствами.

Однако не все государства могут участвовать в этом конкурсе на равных. У стран с более высоким уровнем концентрированных НИОКР в цифровых отраслях и надежных образовательных систем больше шансов управлять общим будущим данных и использовать частный сектор для создания глобальных норм, чем у стран, у которых нет этих показателей. Точно так же, не обладая возможностями инфраструктурной сети, делающей возможной цифровую деятельность, государство находится в неравном положении с более крупными игроками, что, в свою очередь, влияет на выбор политики, отражающей различия в подходах к управлению данными. Более того, режимы

данных также зависят от способности государства функционально управлять своими законами последовательным и предсказуемым образом. Подобно развитию инфраструктуры, страна с законодательными инициативами по влиянию на цифровое пространство может не достичь своей цели, не имея возможности обеспечить соблюдение своих законов или надлежащим образом сбалансировать частные и общественные интересы. Следовательно, это может негативно повлиять на репутацию страны в плане цифрового влияния и, следовательно, поможет учесть расхождения в режимах данных.

Наконец, любая основа для понимания того, как правительства регулируют данные, должна учитывать лидерство и власть. Страны могут играть ведущую роль в создании цифровых норм и проецировании цифровой власти. Лидерство происходит как от дипломатической ловкости, так и от военной силы. Военная мощь касается не только способности государств агрессивно атаковать ключевые активы с помощью кибервойны, но и способности защищать и сдерживать иностранное влияние. Такие способности подразумевают экзистенциальные проблемы общества, поскольку экономики повсюду становятся все более зависимыми от цифровых технологий. Поскольку мир продолжает дробиться, понимание того, где и как страны расходятся в своих интересах, станет ключом к выявлению и предотвращению широко распространенного злоупотребления технологиями, пагубной глобальной конкуренции за власть и усиления международной напряженности. Мы надеемся, что концептуальная призма режимов данных поможет решить эти проблемы.

Ссылки

Адам Пржеворски, Капитализм и социал-демократия (Кембридж: издательство Кембриджского университета,

1986).

Акеми Сузуки и Томохиро Секигучи, «Защита данных и конфиденциальность» Нагашима Оно и

Цунемацу. (2019). https://gettingthedealthrough.com/area/52/juriscohol/36/data-protection-privacy-japan/

Алена Епифанова. «Расшифровка российского« суверенного закона об Интернете »» №2. Немецкий совет по

Международные отношения (январь 2020 г.). https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

Александр Вендт. Социальная теория международной политики (Кембридж: Кембриджский университет

Press, 1999).

Энн Нельсон. «Параллельные миры Кубы: цифровые медиа преодолевают пропасть», Центр

Международная помощь СМИ (август 2016 г.)

Анупам Чандер и Юен П. Ле. «Национализм данных». Юридический журнал Эмори, Vol. 64 (ноябрь

2015), стр. 677-739.

Ариндраджит Басу и др. «Гамбит локализации» Центр Интернета и общества, Индия.

99

(Март 2019 г.), https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf

Айкут Атали, Чандра Гнанасамбандам и Бхаргс Шриватсан. «Преобразование инфраструктуры

Операции для мира гибридных облаков. McKinsey & Company (октябрь 2019 г.) https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/transforming-infrastructure-operations-for-a-hybrid-cloud-world#

Барбара Л. Кон, «Управление данными: императив качества в эпоху больших данных, открытых данных и не только». Журнал права и политики информационного общества Vol. 10, No. 3 (2015), pp. 811-826.

Бенджамин М. Дженсен, Брэндон Валериано и Райан Мэнесс. Киберстратегия: эволюционирующий характер власти и принуждения (Оксфорд: Oxford University Press, 2018).

Берил. А. Радин. «Инструменты межгосударственного управления». Справочник по государственному управлению (Лондон: Sage 2003).

Кэрол Пейтман. Участие и теория демократии (Кембридж: издательство Кембриджского университета, 1970).

Кэтрин Такер. «Сетевые эффекты и рыночная власть: чему мы научились за последнее десятилетие?» Антимонопольное (2018). http://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf

Кристофер Фостер и Шамел Азме. «Новые экономики и национальная цифровая политика: перспектива промышленной политики». Журнал исследований развития (ноябрь 2019 г.).

Дэн Сеньор и Сол Сингер. Нация стартапов: история экономического чуда Израиля (Нью-Йорк: двенадцать, 2009 г.).

Дэниел Дж. Соловье и Пол М. Шварц. Основы законодательства о конфиденциальности. (2015).

Даниэль Троттье и Кристиан Фукс. «Теоретические основы социальных сетей, политики и государства». Социальные сети, политика и государство: протесты, революции, беспорядки, преступность и полицейская деятельность в эпоху Facebook, Twitter и Youtube. (Нью-Йорк: Рутледж 2014).

Дэни Родрик. «Политическая экономия торговой политики». Справочник по международной экономике Vol. 3 (1995), стр. 1457-1494.

Эйлин Донахью и Меган Макдаффи Мецгер, «Искусственный интеллект и права человека», журнал демократии, Vol. 30, No. 2 (апрель 2019).

Г. Уильям Домхофф. Кто правит Америкой? (Верхняя река Сэдл: Прентис-Холл 1967).

Грейс Кисер и Йоан Манта. «Global AI Talent Report 2019». Jfgagne. (Апрель 2019 г.). https://jfgagne.ai/talent-2019/

Ха-Джун Чанг, «Взбивая по лестнице: стратегия развития в исторической перспективе» (Нью-Йорк: Anthem Press, 2003);

Гарри Экштейн. Разделение и сплоченность в демократии (Princeton: Princeton University Press, 1966).

Джорджио Агамбен, Homo Sacer: Суверенная власть и голая жизнь (1995).

Джованни Арриги. Долгий двадцатый век (Нью-Йорк: Verso 1994).

Иммануил Валлерстайн, Современная мировая система. (Кембридж: издательство Кембриджского университета, 1974);

Дж. В. Хендерсон. Глобализация высокотехнологичного производства. (Лондон: Рутледж 1989).

Джагдиш Бхагвати, Правин Кришна и Арвинд Панагария. «Мировая торговая система: тенденции и

Проблемы ». Представлено на Конференции по торговле и флагу: изменение баланса сил в многосторонней торговой системе (2014 г.).

Джеффри Динг. «Расшифровка китайской мечты об ИИ». Институт будущего человечества (март 2018 г.).

Джоэл С. Мигдал. Государство в обществе (Кембридж: Издательство Кембриджского университета 2012).

Джон Х. Честнат. «Развертывание широкополосной связи в США и в Европе: что говорят данные?» Центр технологий, инноваций и конкуренции (июнь 2014 г.).

Джозеф Най. Мягкая сила: средства к успеху в мировой политике, (Нью-Йорк: PublicAffairs 2004).

Йозеф Шумпетер. Капитализм, социализм и демократия (Нью-Йорк: Harper & Brothers 1943).

Джастин Фендос. «Уроки вспышки COVID-19 в Южной Корее: хорошее, плохое и уродливое».

Дипломат (март 2020 г.). https://thediplomat.com/2020/03/lessons-from-south-koreas-covid-19-outbreak-the-good-bad-and-ugly/

Юрген Хабермас. Кризис легитимации (Бостон: Beacon Press 1973).

100

Каришма Банга и Дирк Виллем те Велде. «Как развивать производство и создавать рабочие места в цифровой экономике: 10 приоритетов политики для Кении». Поддержка экономических преобразований (ноябрь 2018 г.).

Кеннет А. Бамбергер и Дейдра К. Маллиган, Конфиденциальность на местах (Кембридж: MIT Press, 2015).

Кенсаку Такасе, «Соответствие GDPR: Закон Японии о защите личной информации».

IAPP (август 2017 г.). https://iapp.org/news/a/gdpr-matchup-japans-act-on-the-protection-of-personal-information/

Клаус Шваб. Четвертая промышленная революция (Новый Южный Уэльс: валюта, 2016).

Ли Джункю. «Структура торговли Кореи и ее политические вызовы». Будущее корейской торговой политики (2012).

Линси Чутел. «Китай экспортирует программное обеспечение для распознавания лиц в Африку, расширяя свою обширную базу данных». Кварц Африка. (Май 2018). https://qz.com/africa/1287675/china-is-exporting-facial-recognition-to-africa-ensuring-ai-dominance-through-diversity/

Маргарет Гроарк, «Власть, действие и структура», Новая политология, Vol. 14, № 1 (1993).

Марк Латонеро, «Управление искусственным интеллектом: защита прав человека», Data & Society (октябрь 2018 г.), https://datasociety.net/wp-content/uploads/2018/10/DataSociety_Governing_Artificial_Intelligence_Upholding_Human_Rights.pdf

Мартина Ф. Ферракане и Хосук Ли-Макияма. «Технологический протекционизм Китая и его необъяснимые основания. Европейский центр международной политической экономии (июнь 2017 г.).

Мартин ван Кревельд. Трансформация войны (Нью-Йорк: Свободная пресса, 1991).

Макс Вебер, «Политика как призвание». Макс Вебер: Очерки социологии, переведенные Е. Х. Гертом и К. Райтом Миллсом (Oxford: Oxford University Press, 1946);

Мельцер, Дж. Лавлок, П. «Регулирование цифровой экономики: понимание важности трансграничных потоков данных в Азии. Институт Брукингса (март 2018 г.).

Мелвин Кранцберг, «Информационный век: эволюция или революция?» в области информационных технологий и социальных преобразований, под редакцией Брюса Гайла (Вашингтон, округ Колумбия: National Academy Press, 1985).

Майкл Чуй и др. «Заметки с рубежа искусственного интеллекта» Глобальный институт McKinsey (сентябрь 2018 г.).

Майкл Манн. Источники социальной власти (Кембридж: издательство Кембриджского университета, 1986).

Ник Срничек, платформенный капитализм (Кембридж: Polity 2016).

Ник Уоллес и Даниэль Кастро. «Влияние нового постановления ЕС о защите данных на ИИ». Центр инноваций в области данных (март 2018 г.).

Нир Хсетри, «Успех краудфандинговых онлайн-технологий в сборе средств: институциональная перспектива». Журнал международного менеджмента, Vol. 21, No. 2. (2015), pp. 101-116.

ОЭСР «Управление данными в государственном секторе», Путь к превращению в государственный сектор, управляемый данными (ноябрь 2019 г.).

Питер Дж. Мэй. «Разработка и реализация политики». Справочник по государственному управлению (Лондон: Sage 2003)

Питер Морган. «Развитие потенциала: введение». Новые проблемы в развитии потенциала: материалы семинара (1993).

Према-чандра Атукорала. «Реформы торговой политики и структура защиты во Вьетнаме». Мировая экономика, Vol. 29. № 2. (2006), стр. 161–187.

Роберт Д. Аткинсон. «Руководство по цифровой инфраструктуре для политиков». Фонд информационных технологий и инноваций (2016).

Роберт А. Даль. Кто правит? (Нью-Хейвен: издательство Йельского университета, 1961 г.).

Роберт Геллман. «Честная информационная практика: базовая история». ССРН (июнь 2019). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

Роберт Райнер. Политика полиции. (Оксфорд: Оксфордский университет, 2010 г.); Кубо Мачак. «Кризис международного права кибербезопасности?» 8-я Международная конференция по кибер-конфликтам, 2016 г., (2016), стр. 132-134.

Росс М. Рустичи. «Кибероружие: выравнивание международного игрового поля». Параметры. (2011).

Райан Хасс и Зак Балин. «Отношения США и Китая в эпоху искусственного интеллекта». Институт Брукингса. (Январь 2019 г.), https://www.brookings.edu/research/us-china-relations-in-the-age-of-artificial-intelligence/;

Сэм Сакс и Джастин Шерман, «Глобальное управление данными: концепции, препятствия и перспективы», Новая Америка (декабрь 2019 г.). https://www.newamerica.org/cybersecurity-initiative/reports/global-data-governance/

101

Скотт Лэш и Джон Урри. Конец организованного капитализма. (Мэдисон: University of Wisconsin Press, 1987), стр. 196-209.

Шон Макдональд и Сяо Мина, Внешняя политика «Истерзанная войной сеть». (Декабрь 2018 г.).

Шаньхун Лю, «Большие данные, статистика и факты», Statista (октябрь 2019 г.). https://www.statista.com/topics/1464/big-data/

Стивен МакНэми и Майкл Глассер. «Концепция власти в социологии: теоретическая оценка». Гумбольдтский журнал социальных отношений, Vol. 15, No. 1. (1987), pp. 79-104.

Стивен П. Маллиган. «Трансграничный обмен данными в соответствии с Законом об облаках». R45173 Исследовательская служба Конгресса. (Апрель 2018).

Стив Макфили и Нур Барнат. «Наращивание статистического потенциала для устойчивого развития: разработка основных принципов, необходимых для современных национальных статистических систем». Европейская экономическая комиссия ООН (ноябрь 2017 г.), стр. 2–4.

Стивен Льюкс. Власть: радикальный взгляд (Лондон: Macmillan, 1974).

Стюарт Фаулер и др. «Разработка политики кибербезопасности, которая распространяется на оборонные закупки Австралии». Журнал Сил обороны Австралии. (2017)

Сьюзан Ааронсон, «Поворот к торговым соглашениям для регулирования Интернета», в работе Jean-Baptise Velut et al. в понимании соглашений о мега-свободной торговле: политическое и экономическое управление нового кросс-регионализма. (Оксфорд: Рутледж, сентябрь 2017 г.);

Стивен Фельдштейн. «Глобальное расширение слежки за ИИ». Фонд Карнеги за международный мир. (Сентябрь 2019 г.).

Тессалено Девезас и др. Индустрия 4.0: предпринимательство и структурные изменения в новом цифровом ландшафте. (Нью-Йорк: Springer, 2016);

Thomas A Singlehurst et al. «Электронная конфиденциальность и защита данных» CitiGroup. (Март 2017 г.).

Тио Цзе Ган, «Защита данных и конфиденциальности в АСЕАН - что это значит для бизнеса в регионе?» Deloitte. (2018);

Том Форестер. Революция информационных технологий. (Кембридж: MIT Press, 1985);

Уилл Эдвардс, «Северная Корея как киберугроза», The Cypher Brief (июль 2016 г.).

Уильям А. Картер и Уильям Д. Крамплер. «Умные деньги на достижениях Китая в области искусственного интеллекта». Центр стратегических и международных исследований (сентябрь 2019 г.).

« Отчет об индексе искусственного интеллекта за 2019 год». Стэнфордский институт искусственного интеллекта, ориентированного на человека (2019), стр. 5, https://hai.stanford.edu/sites/default/files/ai_index_2019_report.pdf

« Коммодификация кибервозможностей: большой базар кибероружия». Программа государственно-частного аналитического обмена 2019. (2019), стр. 14-18.

« Противостояние кризису глобального управления». Отчет Комиссии по глобальной безопасности, правосудию и управлению (июнь 2015 г.).

« Локализация данных: вызов глобальной торговле и свободному потоку информации». Группа Олбрайт Стоунбридж (сентябрь 2015 г.), стр. 12-15. https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf

« Цифровая глобализация: новая эра глобальных потоков». Институт McKinsey. (Март 2016 г.).

https://www.the-digital-insurer.com/wp-content/uploads/2016/06/709-mgi_digital_globalization.pdf

« Глобальные уроки из проблем Дурбана, связанных с изменением климата». Новый гуманитарный. (Май 2011 г.).

http://www.thenewhumanitar.org/news/2011/05/24/global-lessons-durban-s-climate-change-challenges

« Global Talent 2021: Как новая география талантов изменит стратегии управления человеческими ресурсами». Oxford Economics. (2020),

https://www.oxfordeconomics.com/Media/Default/Thought%20Leadership/global-talent-2021.pdf;

« Глобальный риск талантов - семь ответов». Всемирный экономический форум (2011), стр. 9.

http://www3.weforum.org/docs/PS_WEF_GlobalTalentRisk_Report_2011.pdf

« Глобальное исследование электросвязи 2019», Ernst & Young (сентябрь 2019 г.), стр. 4.

https://www.ey.com/Publication/vwLUAssets/ey-accelerating-the-intelligent-enterprise/$FILE/ey-accelerating-the-intelligent-enterprise.pdf

« Глобализация в переходный период: будущее торговли и цепочек создания стоимости». Глобальный институт McKinsey. (Январь 2019), стр. 14.

https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/Globalization%20in%20transition%20The%20future%20of%20trade%20and%20value%20chains/MGI-Globalization-in-transition- Краткий обзор будущего торговли и цепочек добавленной стоимости.pdf

« Государственный индекс готовности к искусственному интеллекту 2019 г.» Oxford Insights (2019 г.), https://www.oxfordinsights.com/ai-readiness2019

« Права человека в эпоху искусственного интеллекта», Access Now (ноябрь 2018 г.)

Белая книга « Как предотвратить дискриминационные результаты в машинном обучении», Всемирный экономический форум (март 2018 г.),

http://www3.weforum.org/docs/WEF_40065_White_Paper_How_to_Prevent_Discriminatory_Outcomes_in_Machine_Learning.pdf

102

« Международные стандарты конфиденциальности». Фонд электронных рубежей. (2018). https://www.eff.org/issues/international-privacy-standards

« Измерение цифровой трансформации: дорожная карта на будущее». ОЭСР (март 2019 г.), стр. 20.

https://www.oecd-ilibrary.org/sites/9789264311992 en / index.html? itemId = / content / publishing / 9789264311992-en

« Национальная стратегия искусственного интеллекта #AIForAll». Нити Аайог. (Июнь 2018 г.),

https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf

« Государство конфиденциальности в Мексике». Privacy International (январь 2019 г.).

https://privacyinternational.org/state-privacy/1006/state-privacy-mexico

« Режим защиты данных в Китае». Генеральный директорат Европейского парламента по международной политике. (2015).

«Ключи к защите данных». Privacy International. (Август 2018),

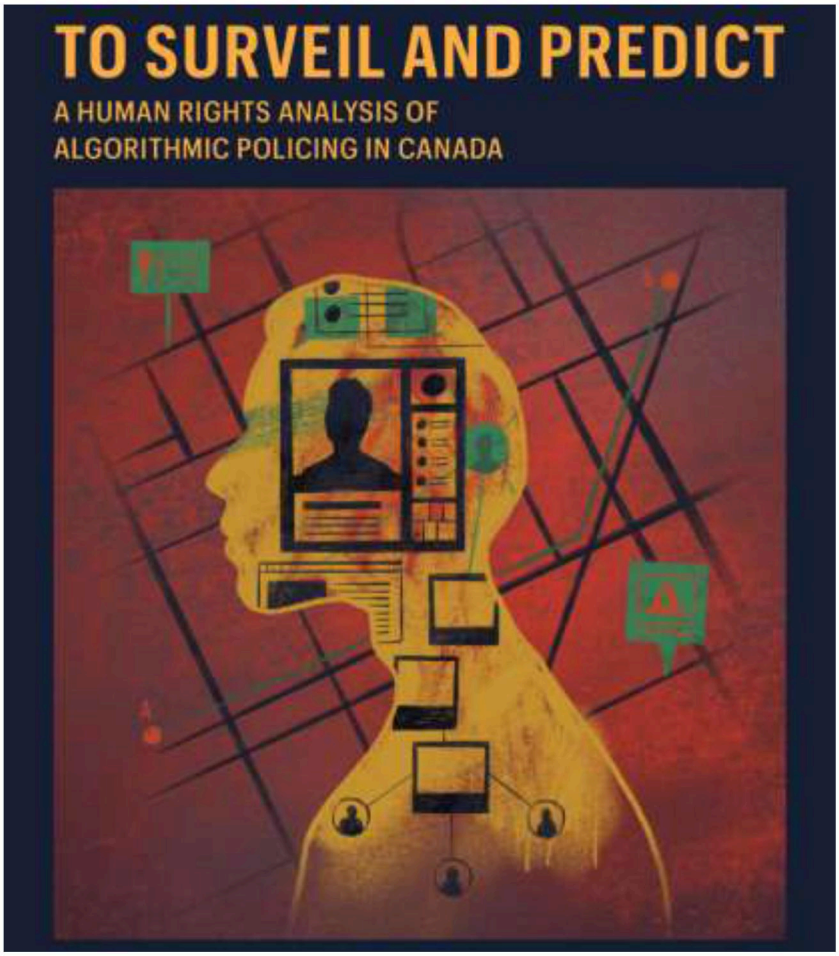
https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf;

«Раскрытие потенциала цифровой экономики Королевства Саудовская Аравия». Эрнст энд Янг, (2019),

https://www.ey.com/Publication/vwLUAssets/ey-unlocking-the-digital-economy-potential-of-the-kingdom-of-saudi-arabia/$File/ey-unlocking-the-digital-economy -потенциал-королевства-саудовской-аравии.pdf

«Раскрытие потенциала экономики данных Индии. Омидьяр Сеть Индия. (Сентябрь 2019 г.),

https://www.omidyarnetwork.in/insights/unlocking-the-potential-of-indias-data-economy-practices-privacy-and-governance



Наблюдать и прогнозировать

Эта публикация является результатом исследования, проведённого международной программой по правам человека Университета Торонто (IHRP) на юридическом факультете и Citizen Lab в школе глобальных дел и государственной политики Мунка.

Авторы: Кейт Робертсон, Синтия Ху и Иоланда Сонг. Руководители исследований: Иоланда Сонг и Синтия Ху. Дизайн и иллюстрации: Юкюн Ким.

Авторское право

© 2020 Citizen Lab (Школа международных отношений и государственной политики, Университет Торонто) и международная правозащитная программа (юридический факультет, Университет Торонто), «вести наблюдение и прогнозировать: по правам человека, анализ алгоритмической деятельности полиции в Канаде», Кейт Робертсон, Синтия Ху, и Иоланда Сонг.

Версия документа: 1.0

Лицензия Creative Commons BY-SA 4.0 (Attribution-ShareAlike License)

Лицензия Creative Commons Attribution-ShareAlike 4.0, в соответствии с которой лицензируется данный отчёт, позволяет вам свободно копировать, распространять, изменять и основываться на нём, пока:

- Признаются интеллектуальные права;
- Указывается вносимые изменения;
- Используется лицензию CC BY-SA 4.0.

Однако любые права на выдержки, воспроизведённые в настоящем отчёте, остаются за их соответствующими авторами, а любые права на названия брендов и продуктов и связанные с ними логотипы остаются за их соответствующими владельцами. Использование этих объектов, защищённых авторским правом или правами на товарные знаки, требует предварительного письменного согласия правообладателя.

Электронная версия впервые опубликована международной программой по правам человека и гражданина в сентябре 2020 года. Доступ к этой работе можно получить через https://ihrp.law.utoronto.ca/ и https://citizenlab.ca.

Благодарности

Международная правозащитная программа и Лаборатория Citizen Lab хотели бы выразить свою искреннюю благодарность за поддержку со стороны многих людей, которые сделали эту работу возможной.

Первичный сбор данных, регламентированный протоколом исследования для данного отчёта, проводился Иоландой Сонг и Синтией Ху.

Этот доклад был подготовлен под руководством профессора Рональда Дейберта.

В докладе был рассмотрен Рональд Джей Дэйберт, профессор политологии и директор Citizen Lab; Кристофер Парсонс, старший научный сотрудник Citizen Lab; Петра Молнар, исполняющая обязанности директора и Самер Мускати, бывший директор ММСП.

Авторы настоящего доклада выражают признательность за дальнейший подробный вклад, руководство и поддержку Кристофера Парсонса.

Авторы выражают огромную благодарность и глубокую признательность за бесценные идеи и советы следующим внешним рецензентам (представленным в алфавитном порядке по фамилиям): Винсенту Чао, адъюнкт-профессору юридического факультета Университета Торонто; Лексу Гиллу, адъюнкту юридического факультета Trudel Johnston & Lesperance и

научному сотруднику Citizen Lab; Тамиру Израэлю, штатному юристу канадской клиники Интернет-политики и общественных интересов Samuelson-Glushko (CIPPIC) Университета Оттавы; Эмили Лам, партнеру юридической фирмы Kastner Law; Бренде Макфейл, директору по конфиденциальности, технологии и наблюдению проекта в Канадской ассоциации гражданских свобод; Ноа Мендельсон-Авива, директору программы равенства в Канадской ассоциации гражданских свобод; Джилл Прессер, основной, главный юрист в юридической школе Осгуд-Холла, адъюнкт-профессор; Рашиде Ричардсон, директору по исследованию политики, ИИ Нью-Йоркского университета; Терезе Скасса, профессору Канадской исследовательской кафедры информационного права и политики в Университете Оттавы, юридический факультет; и Валери Стивз, профессору факультета социальных наук Университета Оттавы, кафедра криминологии.

Этот отчёт был отредактирован Джойсом Парсонсом, директором отдела редактирования и консультирования. Проверила Машока Маймона, студентка юридического факультета Университета Торонто. Обложку и дизайн для доклада завершил Рюкюнг Ким.

Авторы особенно хотели бы поблагодарить студентов юридического факультета Университета Торонто Джули Левенштейн и Соломона Маккензи за их ценную исследовательскую помощь на протяжении всего этого проекта, а также студентку юридического факультета Индию Аннамантаду за её вклад.

Авторы также выражают благодарность многочисленным специалистам по предметной области и заинтересованным экспертам, которые предоставили своё мнение, обратную связь и время для разработки настоящего доклада в ходе неофициальных консультаций с авторами и официальных исследовательских интервью. Авторы также выражают глубокую признательность участникам симпозиума «автоматизированное принятие решений в системе уголовного правосудия», организованного в марте 2019 года совместно с юридической комиссией Онтарио, лабораторией Citizen Lab, IHRP и Ассоциацией адвокатов по уголовным делам, за их участие и взгляды на вопросы, поднятые в настоящем докладе.

Лаборатория Citizen Lab хотела бы поблагодарить следующих спонсоров за поддержку этого исследования: фонд Джона Д. и Кэтрин Т. Макартур, фонд Сигрид Раузинг, фонд Форда и фонд Оука. Это исследование было также частично поддержано грантом фонда «Открытое общество».

Международная программа по правам человека (IHRP) хотела бы поблагодарить юридический фонд Онтарио за поддержку этого исследования.

Об авторах

Кейт Роберсон - адвокат по уголовным делам в юридической фирме «Марксон» в Торонто и научный сотрудник Citizen Lab. Её практика защиты по уголовным делам включает как судебную, так и апелляционную работу, фокусируясь на ряде уголовных дел, включая преступления белых воротничков, сексуальные преступления и компьютерные расследования и преступления. Ранее она работала прокурором провинции Онтарио и клерком в Верховном суде Канады. Она имеет степень доктора юридических наук в Университете Торонто.

Синтия Ху – научный сотрудник лаборатории технологии и права, адвокат по правам человека. Она имеет степень магистра права и технологии (концентрация в области права и технологии) из Университета Оттавы, стажировалась в качестве студента-исследователя и младшего юрисконсульта в канадской клинике Интернет-политики и общественных интересов имени Самуэльсона-Глушко. Её работа охватывает ключевые области законодательства и политики в области цифровых прав, включая неприкосновенность частной жизни, надзор, ответственность посредников, свободу выражения мнений, равенство и злоупотребление технологиями.

Иоланда Сонг – адвокат по гражданским спорам в компании Stevenson Whelton LLP в Торонто. Её практика включает в себя государственное судопроизводство и общее административное и конституционное право. Иоланда работала научным сотрудником в международной программе по правам человека Уильяма Грэма в Университете Торонто, факультет права, и она продолжает работать в качестве научного сотрудника pro bono для IHRP. Она имеет степень доктора юридических наук в Университете Торонто.

О международной программе по правам человека

Международная программа по правам человека (IHRP) на юридическом факультете Университета Торонто решает наиболее насущные проблемы прав человека двумя путями: программа освещает вопиющие нарушения прав человека с помощью докладов, публикаций и информационно-пропагандистской деятельности, а также предлагает студентам беспрецедентные возможности для совершенствования своих юридических исследований и адвокатских навыков с помощью проектов юридических клиник и глобальных стипендий. Фундаментальным приоритетом IHRP является воздействие: программа стремится вооружить студентов и недавних

выпускников навыками, знаниями и профессиональной связи, чтобы стать эффективными защитниками прав человека. Программа также направлена на борьбу с нарушениями прав человека в Канаде и за рубежом путём проведения всесторонних исследований и пропаганды, направленных на реформирование законодательства, политики и практики.

О Citizen Lab

Citizen Lab – это междисциплинарная лаборатория, базирующаяся в школе глобальных дел и государственной политики Мунка Университета Торонто, специализирующаяся на исследованиях, разработках и стратегическом политическом и правовом взаимодействии высокого уровня на пересечении информационно-коммуникационных технологий, прав человека и глобальной безопасности. Лаборатория Citizen Lab использует «смешанные методы» в исследованиях, объединяя практики из политологии, юриспруденции, информатики и регионоведения. Наше исследование включает в себя: исследование цифрового шпионажа против гражданского общества; документирование интернет-фильтрации и других технологий и практик, влияющих на свободу выражения мнений в интернете; анализ конфиденциальности, безопасности и информационного контроля популярных приложений; а также изучение механизмов прозрачности и подотчётности, имеющих отношение к взаимоотношениям между корпорациями и государственными органами в отношении персональных данных и других видов надзорной деятельности.

Замечания и вопросы

Пожалуйста, присылайте все вопросы и исправления авторам непосредственно по адресу:

kate@citizenlab.ca

cynthia@citizenlab.ca

yolanda.song@utoronto.ca

Список аббревиатур

ИИ	Искусственный интеллект
АОВ	Алгоритмическая оценка воздействия
АРНЗ	Автоматическое распознавание номерных знаков
СВЗК (CCTV)	Система видеонаблюдения замкнутого контура
(COMPAS)	Профилирование управления исправительными учреждениями для альтернативных санкций
КПИЦ	Канадский полицейский информационный центр
ПУЧ	Полицейское управление Чикаго
ПСК	Полицейская служба Калгари
КОРСМ	Консолидированные отчёты и разведывательная среда майнинга (Ванкувер, БК)
ИСК	Исправительная служба Канады
СИД	Система информирования о домене (Нью-Йорк)
СЦР	Сеть цифрового распознавания
ЦГИ	Центр города Истсайд (Ванкувер, БК)
ПСЭ	Полицейская служба Эдмонтона
СПП(Э)	Справедливость, подотчётность прозрачность (и этика)
ИПНПУД	Инициатива первых наций по управлению данными
СИ	Свобода информации
ОПЗД	Общие правила защиты данных (Европейский Союз)
GeoDASH	Центр анализа и статистики географических данных (Ванкувер, БК)
GeoDASH APS	GeoDASH Системы алгоритмической деятельности полиции (Ванкувер, БК)
GPS	Глобальная система позиционирования
ИОРПВ	Инструмент оценки риска причинения вреда (Дарем, Великобритания)
HRIA	Оценка воздействия на права человека

МКППЧ	Межамериканская комиссия по правам человека
МПОГИПП	Международный пакт о гражданских и политических правах
МИМА	Международная идентификация мобильного абонента
ПУЛА	Полицейское управление Лос-Анджелеса
СДВЛА	Стратегическая добыча и восстановление Лос-Анджелеса
ИУО	Инвентаризация уровня обслуживания
МО	Машинное обучение
УКППЧ	Управление Комиссара по правам человека (Организация Объединенных Наций)
ОПСОЦ	Оттавский полицейский стратегический оперативный центр
ОВНЧЖ	Оценка воздействия на частную жизнь
ЗОЗПДИЭД	Закон о защите персональных данных и электронных документах
ЛПИ	Лицо, представляющее интерес
СУИОПЗ-БК	Среда управления информацией о полицейских записях - Британская Колумбия
КККП	Королевская Канадская конная Полиция
СУЗ	Система управления записями
БДОР	База данных отслеживания рисков
АСС	Анализ социальных сетей
ЛПАПС	Лаборатория прогнозной аналитики Саскачевана
ПСС	Полицейская служба Саскатуна
СПДСН	Статистический пакет для социальных наук
ССТ	Список стратегических тем (Чикаго, Иллинойс)
ПСТ	Полицейская Служба Торонто
ДПВ	Департамент Полиции Ванкувера

Основные положения

В настоящем докладе рассматриваются алгоритмические технологии, предназначенные для системного использования в уголовном правоприменении. Алгоритмическая политика – это область технологического развития, которая теоретически предназначена для того, чтобы позволить правоохранительным органам либо автоматизировать наблюдение, либо делать выводы с помощью массовой обработки данных в надежде предсказать потенциальную преступную деятельность. Последний тип технологии и методы контроля, основанные на нём, часто называют прогнозирующим контролем. Алгоритмические методы полицейской деятельности часто основываются на агрегировании и анализе огромных объёмов данных, таких как личная информация, коммуникационные данные, биометрические данные, данные геолокации, изображения, контент социальных сетей и данные полицейской деятельности (например, статистические данные, основанные на полицейских арестах или уголовных делах).

Для того, чтобы направлять общественный диалог и развитие законодательства и политики в Канаде, в докладе основное внимание уделяется последствиям использования правоохранительными органами алгоритмических полицейских технологий в области прав человека и конституционного права. В настоящем докладе впервые излагаются методология и объём анализа в части 1.

В части 2 доклада рассматриваются важнейшие социальные и исторические контексты, касающиеся системы уголовного правосудия в Канаде, включая вопросы, касающиеся системной дискриминации в системе уголовного правосудия и предвзятости в массивах данных полиции. Этот социально-исторический контекст важен для понимания того, каким образом алгоритмические полицейские технологии создают повышенные риски нанесения ущерба гражданским свободам и связанным с ними проблемам в области прав человека и конституционного права для определённых лиц и сообществ. Используемые полицией генерируемые наборы данных, подверженные системному смещению, могут создавать циклы отрицательной обратной связи, когда люди из исторически неблагополучных сообществ помечаются алгоритмом как повышенный риск из-за исторического смещения в сторону этих сообществ.

Затем в части 3 доклада приводится несколько концептуальных строительных блоков для организации дискуссии вокруг технологии алгоритмической полицейской службы, и в ней описываетсятехнология алгоритмической полицейской службы отличается от традиционных методов полицейской службы.

В части 4 доклада излагаются и обобщаются выводы о том, как правоохранительные органы Канады начали использовать, закупать, разрабатывать или тестировать различные алгоритмические методы полицейской деятельности. В докладе собраны оригинальные исследования с существующими исследованиями, чтобы дать всесторонний обзор того, что известно об алгоритмическом ландшафте полицейской деятельности в Канаде на сегодняшний день.

В обзоре использования алгоритмической полицейской технологии в Канаде в докладе приводится классификация алгоритмических полицейских технологий по следующим трём категориям:

- Ориентированные на местоположение алгоритмические полицейские технологии – это подмножество того, что имеет в целом известность, как технологии «предсказательной полиции». Эта категория технологии алгоритмической полиции направлена на то, чтобы определить, где и когда потенциально может возникнуть преступная деятельность. Алгоритмы, управляющие этими системами, исследуют корреляции в исторических полицейских данных для того, чтобы попытаться сделать прогнозы о заданном наборе географических областей.
- Личностно-ориентированные алгоритмические полицейские технологии также являются подмножеством прогнозных полицейских технологий. Ориентированные на личность алгоритмические полицейские технологии опираются на анализ данных для того, чтобы попытаться идентифицировать людей, которые с большей вероятностью будут вовлечены в потенциальную преступную деятельность, или оценить идентифицированное лицо на предмет предполагаемого риска вовлечения в преступную деятельность в будущем.
- Личностно-ориентированные алгоритмические полицейские технологии также являются подмножеством прогнозных полицейских технологий. Ориентированные на личность алгоритмические полицейские технологии опираются на анализ данных для того, чтобы попытаться идентифицировать людей, которые с большей вероятностью будут вовлечены в потенциальную преступную деятельность, или оценить идентифицированное лицо на предмет предполагаемого риска вовлечения в преступную деятельность в будущем. Технологии полицейского алгоритмического наблюдения, как они называются в настоящем докладе, по своей сути не включают никакого прогностического элемента и, таким образом, отличаются от двух вышеперечисленных категорий (ориентированная на местоположение и ориентированная на человека алгоритмическая политика). Скорее, алгоритмические технологии наблюдения предоставляют полицейским службам сложные, но общие функции наблюдения и мониторинга. Эти технологии автоматизации

систематического сбора и обработки данных (такие данные как, собранные в интернете, или изображения, снятые с физически открытых пространств). Некоторые из этих технологий (например, технология распознавания лиц, которая обрабатывает фотографии из баз данных mug-shot) могут по-новому обрабатывать данные, которые уже хранятся в полицейских досье правоохранительных органах. Для удобства использования этот набор технологий будет называться просто технологией алгоритмического наблюдения на протяжении всей остальной части настоящего доклада. Этот термин следует понимать в ограниченном контексте полицейской деятельности (таким образом, исключая другие формы алгоритмических технологий наблюдения, которые более тесно связаны с другими контекстами, такими как соблюдение налогового законодательства или наблюдение за получателями социального обеспечения).

Основные результаты исследований, содержащиеся в настоящем докладе, показывают, что технологии были закуплены, разработаны и внедрены, или используются в Канаде во всех трёх категориях. Например, по меньшей мере два ведомства, Департамент полиции Ванкувера и полицейская служба Саскатуна, подтвердили, что они используют или разрабатывают «прогностические» алгоритмические технологии в целях руководства действиями и вмешательством полиции. Другие полицейские службы, например, в Калгари и Торонто, приобрели технологии, которые включают в себя возможности алгоритмической полицейской деятельности или которые используются юрисдикциями за пределами Канады для создания прогнозных полицейских систем. Полицейская служба Калгари занимается алгоритмическим анализом социальных сетей, который является одной из форм технологии, которая также может быть использована правоохранительными органами для участия в ориентированной на человека алгоритмической полиции. Многочисленные правоохранительные органы по всей стране также в настоящее время полагаются на ряд других алгоритмических технологий наблюдения (например, автоматизированные считыватели номерных знаков, распознавание лиц и алгоритмы наблюдения за социальными сетями), либо они разрабатывают или рассматривают возможность внедрения таких технологий. Этот отчёт также раскрывает информацию, предполагающую, что провинциальная Полиция Онтарио и региональная полицейская служба Ватерлоо могут незаконно перехватывать частные сообщения в онлайн-частных чатах, полагаясь на алгоритмическую технологию наблюдения за социальными сетями, известную как система онлайн-защиты детей ICAC (ICACCOPS). Другие полицейские службы по всей Канаде также могут использовать или разрабатывать дополнительные прогностические полицейские или алгоритмические технологии наблюдения за пределами осведомлённости общественности. Многие запросы о свободе информации (FOI),

представленные для настоящего доклада, были встречены ответами правоохранительных органов, которые требовали привилегий в качестве оправдания неразглашения; в других случаях правоохранительные органы не предоставляли никаких записей в ответ на представленный запрос FOI или запрашивали непомерные гонорары за обработку запроса.

Основываясь на выводах о текущем состоянии алгоритмической полиции в Канаде, в части 5 доклада представлен правозащитный и конституционно-правовой анализ потенциального использования алгоритмических полицейских технологий. Правовой анализ применяет установленные правовые принципы к этим технологиям и демонстрирует, что их использование правоохранительными органами может привести к нарушению основных прав и свобод человека, которые охраняются канадской Хартией прав и свобод (далее Хартия) и международными правами человека. В частности, авторы анализируют потенциальное воздействие алгоритмических полицейских технологий на следующие права: право на неприкосновенность частной жизни; право на свободу выражения мнений, мирных собраний и ассоциаций; право на равенство и свободу от дискриминации; право на свободу и свободу от произвольного задержания; право на надлежащую правовую процедуру и право на средства правовой защиты.

Основные выводы этого анализа представлены следующим образом:

- Последствия для права на неприкосновенность частной жизни и права на свободу выражения мнений, мирных собраний и объединений: растущее использование алгоритмических технологий наблюдения в Канаде угрожает неприкосновенности частной жизни и основным свободам выражения мнений, мирных собраний и объединений, которые защищены Хартией и международным правом человека. Расширенные возможности и повышенные требования к данным алгоритмических полицейских технологий вводит новые угрозы частной жизни и этим основным свободам, такие как при перепрофилировании исторических полицейских данных конституционно сомнительные данные механизмы совместного использования, или в алгоритмическом наблюдении за общественными собраниями, или онлайн-выражение, повышающее значительные риски нарушений. Канадская правовая система в настоящее время не имеет достаточно чётких и надёжных гарантий для обеспечения того, чтобы использование алгоритмических методов наблюдения, если таковые имеются, происходит в рамках конституционных границы и подчиняется необходимым нормативным, судебным и законодательным актам. Учитывая потенциальный ущерб, который может

нанести неограниченное использование алгоритмического наблюдения со стороны правоохранительных органов основным свободам и свободному обществу, использование таких технологий в отсутствие надзора и соблюдения ограничений, определённых необходимостью и соразмерностью, является неоправданным.

Последствия для права на равенство и свободу от дискриминации:

- Системный расизм в канадской системе уголовного правосудия должен лежать в основе любого анализа алгоритмической полицейской деятельности, особенно ее воздействия на маргинализованные общины. Кажущееся «нейтральным» применение алгоритмических инструментов контроля маскирует реальность, так что они могут непропорционально сильно воздействовать на маргинализованные общины в защищённом категория в соответствии с законом «О равенстве» (т. е. сообщества, основанные на таких характеристиках, как раса, этническая принадлежность, сексуальная ориентация или инвалидность). Социально исторический контекст системной дискриминации влияет на надежность наборов данных, которые уже удерживаемые правоохранительными органами (например, данные об арестах и преступлениях учётная документация). Многочисленные неточности, предубеждения и другие источники недостоверности присутствуют в большинстве распространенных источников полицейских данных в Канаде. Как результат - составление непредвзятых и надёжных выводов на основе исторических полицейских данных это - по всей вероятности, невозможно. Перед законом необходимо проявлять крайнюю осторожность правоохранительным органам, если вообще разрешено, использовать технологии алгоритмической полиции, которые обрабатывают массивы полицейских данных. В противном случае эти технологии могут усугубить и без того неконституционные и разрушительные последствия систематического преследования маргинализированных общин.

Последствия для права на свободу от произвольного задержания: полагаться на алгоритмическое прогнозирование для оправдания вмешательства в свободу личности несовместимо с конституционным правом и правом человека. По определению, методы алгоритмического контроля обычно приводят к обобщённым выводам. В соответствии с законом о правах человека и Уставом потеря свободы (например, задержание, арест, отказ в освобождении под залог и наказание в виде приговора) не может быть оправдана на обобщённых или стереотипных предположениях, таких как подозрение, основанное на представления об этнической группе или о месте, где был

найден индивид. Использование алгоритмических полицейских технологий для оправдания вмешательства в свободу может нарушать права Хартии, когда предполагаемые основания для вмешательства в свободу основаны на алгоритмических прогнозах, полученных на основе статистических тенденций, а не конкретизируются для конкретного человека. Нарушения могут включать случаи, когда человек не был бы задержан или арестован, если бы не наличие алгоритмического прогноза, основанного на статистических тенденциях, при прочих равных обстоятельствах.

В дополнение к этим основным выводам в докладе документируются проблемы, которые, вероятно, возникнут в отношении реального доступа к правосудию и прав на надлежащую правовую процедуру и средства правовой защиты, учитывая, что эффективные механизмы подотчетности для алгоритмических полицейских технологий часто отсутствуют, а также в свете системных проблем, с которыми сталкиваются отдельные лица и общины, стремящиеся получить реальную компенсацию за нарушения прав, которые не приводят к обвинениям в канадских судах. Отсутствие столь необходимой прозрачности в канадском алгоритмическом полицейском ландшафте оживляет многие из основных рекомендаций, содержащихся в этом докладе. Авторы надеются, что этот доклад даст представление о критической необходимости прозрачности и подотчётности в отношении того, какие типы технологий в настоящее время используются или разрабатываются и как эти технологии используются на практике. Располагая уточнённой информацией о том, что в настоящее время используется и разрабатывается, политики и законодатели могут позволить общественности и правительству наметить обоснованный путь вперёд.

В ответ на выводы, сделанные на основе юридического анализа, доклад заканчивается рядом рекомендаций для правительств и правоохранительных органов в целях разработки законодательства и надзора, которые устанавливали бы необходимые ограничения на использование алгоритмических полицейских технологий. В части 6 приводится перечень этих рекомендаций, каждая из которых сопровождается контекстуальной информацией, разъясняющей цель рекомендации и предлагающей потенциальные руководящие указания по её осуществлению. Эти рекомендации подразделяются на приоритетные рекомендации, которые должны быть выполнены сейчас, в срочном порядке, и вспомогательные рекомендации, которые могут быть неприменимы в тех случаях, когда определённые технологии алгоритмического контроля запрещены, но должны быть реализованы, если какие-либо технологии должны быть разработаны или приняты. Ниже приводится краткое резюме этих рекомендаций:

A. Приоритетные рекомендации для правительств и правоохранительных органов, которые необходимо срочно принять для снижения вероятности нарушений прав человека и Хартии, связанных с использованием алгоритмических полицейских технологий в Канаде:

1. Правительства должны ввести мораторий на использование правоохранительными органами технологий, основанных на алгоритмической обработке исторических массивов данных массовой полиции, до завершения всеобъемлющего обзора в рамках судебного расследования, а также на использование алгоритмических полицейских технологий. Это не соответствует предварительным условиям надёжности, необходимости и пропорциональности.

2. Федеральное правительство должно созвать судебное расследование для проведения всеобъемлющего обзора возможностей правоохранительных органов по перепрофилированию исторических наборов полицейских данных для использования в алгоритмических полицейских технологиях.

3. Правительства должны сделать надёжность, необходимость и соразмерность обязательными условиями для использования алгоритмических полицейских технологий, необходимо ввести мораторий на каждую алгоритмическую полицейскую технологию, которая не соответствует этим установленным предпосылкам.

4. Правоохранительные органы должны быть полностью прозрачными с общественностью и с уполномоченными по вопросам конфиденциальности, немедленно раскрывая, используются ли и какие алгоритмические полицейские технологии в настоящее время, разрабатываются или закупаются, чтобы обеспечить демократический диалог и значимую подотчётность.

5. Правительствам провинций следует принять директивы, касающиеся использования и закупок алгоритмических полицейских технологий, включая требования о том, что правоохранительные органы должны проводить оценку алгоритмического воздействия до разработки или использования любой алгоритмической полицейской технологии; публиковать ежегодные публичные отчёты, раскрывающие подробную информацию о том, как используются алгоритмические полицейские технологии, включая информацию о любых связанных с ними данных, таких как источники учебных данных, потенциальные искажения данных, а также входные и выходные данные, где это применимо; а также содействовать и публиковать независимые экспертные оценки и научную валидацию любой такой технологии до её использования.

6. Правоохранительные органы не должны бесконтрольно использовать алгоритмические полицейские технологии в общественных местах: полицейские службы должны запретить полагаться на алгоритмические предсказания для оправдания вмешательства в личную свободу и должны получить предварительное судебное разрешение перед развёртыванием алгоритмических средств наблюдения на общественных собраниях и в онлайн-среде.

7. Правительства и правоохранительные органы должны привлекать внешних экспертов, в том числе из исторически маргинализированных общин, которые непропорционально страдают от системы уголовного правосудия, до и при рассмотрении, разработке или принятии алгоритмических полицейских технологий, при разработке соответствующих механизмов регулирования и надзора, в рамках завершения оценки алгоритмического воздействия и при мониторинге воздействия алгоритмических полицейских технологий, которые были введены в действие, если таковые имеются.

B. Дополнительные рекомендации для правоохранительных органов:

1. Правоохранительным органам следует укреплять целостность полицейских баз данных и практику управления ими, включая укрепление способности отдельных лиц проверять и корректировать точность личной информации, хранящейся в полицейских базах данных.

2. Правоохранительные органы должны проявлять крайнюю осторожность, чтобы предотвратить неконституционную практику обмена данными с частным сектором и другими неполицейскими государственными субъектами.

3. Правоохранительные органы должны применять следующую передовую практику всякий раз, когда алгоритмическая полицейская технология была или будет принята, или введена в действие в отношении этой технологии:

I. Внедрить постоянные механизмы отслеживания для мониторинга потенциальной предвзятости при использовании любой алгоритмической полицейской технологии;

II. Привлечение внешних экспертов на постоянной основе, включая консультации с сообществами и отдельными лицами которые систематически маргинализируются системой уголовного правосудия, о потенциальном или продемонстрированном воздействии на них алгоритмической полицейской технологии;

III. Формально документировать письменную политику, связанную с использованием алгоритмической полицейской технологии;

IV. Внедрить механизмы ревизии в рамках полицейских служб для укрепления и выявления передовой практики и областей, требующих совершенствования с течением времени.

C. Вспомогательные рекомендации по реформе законодательства и связанным с этим мерам со стороны федеральных, провинциальных, территориальных и муниципальных органов власти:

1. Федеральному правительству следует реформировать положения Уголовного кодекса, касающиеся судебных ордеров, с тем, чтобы конкретно рассмотреть вопрос об использовании правоохранительными органами алгоритмических полицейских технологий.

2. Федеральные и провинциальные законодательные органы должны пересмотреть и модернизировать законодательство о неприкосновенности частной жизни с уделением особого внимания переоценке существующих гарантий с учётом передовых возможностей алгоритмических полицейских технологий и сохранению и уничтожениюбиомтерических данных правоохранительными органами.

3. Федеральному правительству следует расширить положения Уголовного кодекса о парламентской отчётности, которые в настоящее время применяются только к определённым методам электронного наблюдения с тем, чтобы конкретно охватить полномочия полиции в отношении использования правоохранительными органами алгоритмических полицейских технологий.

4. Правительства должны обеспечить, чтобы уполномоченные по вопросам неприкосновенности частной жизни и прав человека были наделены полномочиями и располагали достаточными ресурсами для инициирования и проведения расследований использования правоохранительными органами алгоритмических полицейских технологий.

D. Вспомогательные рекомендации для правительства по обеспечению доступа к правосудию в связи с воздействием алгоритмической полицейской технологии на права человека:

1. Правительствам следует выделять финансовые средства на проведение исследований в целях повышения доступности независимых экспертных знаний.

2. Правительства должны обеспечить адекватную помощь малообеспеченным и незащищённым обвиняемым с тем, чтобы они могли привлекать экспертов – свидетелей в уголовном судопроизводстве.

3. Правительства и правоохранительные органы должны сделать исходный код алгоритмической полиции технологии общедосьупным или, в соответствующих случаях, конфиденциально доступным для государственных органови независимых экспертов для целей оценки алгоритмического воздействия, предварительного обзора закупок, тестирования безопасности, аудита, расследований и судебных разбирательств.

1. Обзор и Предыстория

Вступление

Алгоритмическая полиция – это область технологического развития, которая теоретически предназначена для того, чтобы позволить правоохранительным органам автоматизировать наблюдение или делать выводы путём массовой обработки данных в надежде предсказать потенциальную преступную деятельность. Последний тип технологии и методы контроля, построенные на нём, часто называют технологией «прогнозного контроля». Вообще говоря, цель алгоритмической полицейской технологии состоит в том, чтобы дополнить традиционные методы полицейского расследования и позволить правоохранительным органам уделять приоритетное внимание использованию ресурсов с тем, чтобы они могли более эффективно предотвращать или выявлять преступления.

Степень, в которой канадские правоохранительные органы начали использовать алгоритмические полицейские технологии, плохо изучена. В этом докладе, во-первых, излагаются результаты исследований о том, как правоохранительные органы Канады начали использовать алгоритмические полицейские технологии, а во-вторых, рассматриваются последствия использования алгоритмов в канадской системе уголовного правосудия для прав человека и конституционного права. Использование алгоритмических технологий полицейскими органами является предметом настоящего доклада, но анализ прав человека и конституционного права также относится к алгоритмическим технологиям, которые могут быть использованы на других этапах системы уголовного правосудия.

В связи с относительно ограниченным общественным использованием алгоритмической полицейской технологии в Канаде, этот отчёт «Наблюдение и прогнозирование: анализ прав человека алгоритмической полиции в Канаде», – предполагает дальновидный подход. В дополнение к анализу алгоритмических полицейских технологий, которые, как известно, используются канадскими полицейскими службами, авторы рассматривают технологии, которые, по их мнению, находятся на горизонте, основываясь на результатах, заявлений, сделанных публично или в исследовательских интервью сотрудниками правоохранительных органов, и внедрении алгоритмических полицейских технологий в коллегиальных юрисдикциях, таких как Соединённые Штаты и Соединённое Королевство.

Этот доклад вносит свой вклад в принятие государственных решений относительно потенциального использования алгоритмических полицейских технологий в Канаде с учётом прав человека и конституционных последствий применения таких технологий в целях обеспечения соблюдения уголовного законодательства. Алгоритмическая полиция поднимает вопросы, которые идут в дополнение к вопросам о том, является ли соответствующая технология полезной, экономически эффективной или надёжной, даже если на такие вопросы нетрудно дать ясный ответ. Уязвимость населения, которое непропорционально страдает от системы уголовного правосудия, требует тщательного подхода к внедрению новых технологий (таких как технологии, которые могут влиять на частоту или форму уличных задержаний, арестов и наблюдения), которые правоохранительные органы могут использовать таким образом, чтобы существенно повлиять на жизнь часто уже маргинализированных лиц. Кроме того, действия государства при расследовании преступлений должны быть ограничены конституционными рамками (хотя на практике правоохранительные органы зачастую не выполняют эту обязанность).[734] В результате крайне важно, чтобы государственные субъекты и лица, принимающие решения на всех уровнях государственного управления и системы уголовного правосудия, критически оценивали потенциал алгоритмических полицейских технологий для нарушения прав, предусмотренных канадской Хартией прав и свобод («Хартия»), а также своих обязательств по международным правам человека.[735] Инициативы алгоритмической полиции затрагивают целый ряд проблем, связанных с гражданскими свободами, связанными с надлежащей правовой процедурой, равенством, неприкосновенностью частной жизни, свободой и другими основными свободами, такими как свобода выражения мнений.

---

[734] История уголовного судопроизводства в Канаде изобилует примерами признанных нарушений конституционных прав отдельных лиц правоохранительными органами (see, e.g., R v Grant, 2009 SCC 32; R v Le, 2019 SCC 34; R v Evans, [1996] 1 SCR 8; R v Nasogaluak, 2010 SCC 6; R v Cole, 2012 SCC 53).

[735] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Канадское правительство признало необходимость ориентированного на права человека подхода к рассмотрению вопроса о том, следует ли интегрировать алгоритмические технологии в услуги государственного сектора или нет.[736]

В Канаде появились законодательные и политические изменения, направленные на решение проблемы пересечения ИИ и прав человека, хотя на момент написания этой статьи ни одно из них конкретно не касалось алгоритмической полиции[737]. Международные учреждения также занимаются изучением последствий использования государствами ИИ для прав человека. В то же время гражданское общество и неправительственные организации обратили срочное внимание на вопросы гражданских свобод, касающиеся справедливости, подотчётности, прозрачности и этики (именуемой судьбой), которые затрагиваются ряд алгоритмических технологий, а также на необходимость утверждения чётких ограничений на использование технологий, необходимых для поддержания Устава и прав человека[738]. Правительственные инициативы в коллегиальных юрисдикциях начали исследовать или регулировать алгоритмические технологии[739].

---

[736] Наиболее заметной инициативой федерального правительства стала работа Казначейского совета Секретариата Канады (TBSC), которая включает Директиву об автоматизированном принятии решений, инструмент оценки алгоритмического воздействия и белую книгу "Ответственный искусственный интеллект в правительстве Канады": Government of Canada, «Directive on Automated Decision-Making» (5 February 2019) <https://www. tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>; Government of Canada, «Algorithmic Impact Assessment (AIA)» (31 May 2019) <https://www.canada. ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html>; Government of Canada, «Responsible Artificial Intelligence in the Government of Canada: Digital Disruption White Paper Series» (10 April 2018).

[737]See, e.g., UN Human Rights Council, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29 (3 Aug 2018) <https://undocs.org/A/HRC/39/29>; UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (29 Aug 2018) <https://undocs.org/AA73/348>; United Nations Office of the High Commissioner of Human Rights, «Expert Seminar on Artificial Intelligence and the Right to Privacy» (May 2020) <https://www.ohchr. org/EN/Issues/Digita lAge/Pages/SeminarArtificialIntelligence.aspx>.

[738] See, e.g., Montreal Declaration Responsible AI, «Montreal Declaration for a responsible development of artificial intelligence» (2018) < https:// www.montrealdeclaration-responsibleai.com>; Access Now, «The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems» (16 May 2018) <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and- non-discrimination-in-machine-learning-systems/>. Generally, the FATE approach has been critiqued due to its propensity to focus on soft governance through ethics, as opposed to regulating hard and necessary limits: see, for example, Campolo, A, Sanflippo, M, Whittaker, M, & Crawford, K, «AI Now Report 2017» (2017), <https://ainowinstitute.org/AI_Now_2017_Report.pdf>, at p 34.

[739] See e.g., United Kingdom Government, «Investigation launched into potential for bias in algorithmic decision-making in society» (20 March 2019) <https://www.gov.uk/government/news/investigation-launched-into-potential-for-bias-in-algorithmic-decision-making-in-society>; Directive (EU) 2016/680 of the European Parliament and of the Council 27 Апреля 2016 года по защите физических лиц в отношении обработки персональных данных компетентными органами в целях предупреждения, расследования, выявления или уголовного преследования уголовных преступлений или исполнения уголовных наказаний, а также о свободном перемещении таких данных, и об отмене Рамочного решения Совета 2008/977/JHA (2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016L0680-20160504>; US Executive Office of the President, Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights (May 2016) https://obamawhitehouse.archives.gov/sites/default/files/microsites/ ostp/2016_0504_data_discrimination.pdf>; Adi Robertson, «A new bill would force companies to check their algorithms for bias», The Verge (10 April 2019) <https://www.theverge.com/2019/4/10/18304960/congress-algorithmic-accountability-act-wyden-clarke-booker-bill-introduced- house-senate>; City of New York, «Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City» (16 May 2018) <https://www1.nyc.gov/office-of-the-mayor/news/251-

На этом фоне канадские политики и руководящие органы имеют возможность возглавлять разработку законов, политики и практики в области алгоритмической полицейской технологии, которые уважают права человека, защищаемые на национальном и международном уровнях. Основываясь на выводах и анализе, приведённых в настоящем докладе, лица, принимающие решения в Канаде, обязаны подходить к алгоритмической полицейской технологии с осторожностью, тщательно оценивая потенциальное воздействие алгоритмической полицейской технологии на права человека и конституционные последствия до её принятия правоохранительными органами Канады. Такие оценки позволят принять надлежащие меры для смягчения или предотвращения нарушений прав человека и причинения ущерба отдельным лицам и общинам, которые в противном случае были бы вызваны продолжающимся использованием или внедрением новых, непроверенных или несовершенных технологий.

В целях информирования и руководства общественным диалогом, правом и разработкой политики настоящий доклад предоставляет общественности и государственным субъектам обзор последствий интеграции алгоритмических полицейских технологий в систему уголовного правоприменения в области прав человека и конституционного права. Таким образом, результаты исследований и анализ, представленные в настоящем докладе, отвечают на два основных вопроса:

1. Используют ли в настоящее время канадские правоохранительные органы, разрабатывают ли они или рассматривают возможность внедрения алгоритмических полицейских технологий, и если да, то каковы детали таких инициатив? Исследование, проведённое для этого отчёта, показало, что многочисленные правоохранительные органы по всей Канаде начали использовать, закупать, разрабатывать или тестировать различные алгоритмические методы полицейской деятельности. Эти программы включают в себя использование и развитие технологий «предсказательной полиции» – ориентированной на одно местоположение и ориентированной на одного человека и использование алгоритмических инструментов наблюдения, таких как технология распознавания лиц и анализ социальных сетей. Кроме того, некоторые правоохранительные органы приобрели инструменты с возможностями алгоритмической полицейской технологии, но в настоящее

18/mayor-de-blasio-first-in-nation-task-force-examine-automated- decision-systems-used-by>; April Glaser, «San Francisco is about to be the first US city to ban police from using facial recognition tech», Slate (6 May 2019) <https://slate.com/technology/2019/05/san-francisco-first-city-ban-facial-recognition.html>; Andy Rosen, «Somerville moves to ban facial recognition surveillance», The Boston Globe (10 May 2019) <https://www.bostonglobe.com/metro/2019/05/10/somerville-moves-ban- facial-recognition-surveillance/ebhl0qcX6k14O1H78yrpiI/story.html>. These initiatives have not all been without criticism, however; see e.g., Rashida Richardson, ed, «Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force», AI Now Institute (December 2019) <https://ainowinstitute.org/ads-shadowreport-2019.pdf>.

время они не используют эту возможность из-за отсутствия интереса на момент написания статьи или отсутствия ресурсов для реализации таких инициатив. Полные результаты исследований в ответ на этот вопрос изложены в части 4 («Алгоритмическая полиция в Канаде: современный ландшафт») настоящего доклада.

2. Каковы последствия использования алгоритмических полицейских технологий для прав человека и конституционного права и рискует ли их использование нарушить конституционные права или права человека? Правовой и политический анализ, проведённый для настоящего доклада, показал, что использование алгоритмических полицейских технологий правоохранительными органами может привести к множеству потенциальных нарушений конституционных и гражданских свобод в соответствии с канадской Хартией прав и свобод и международных прав человека. В частности, анализ выявил ряд проблем, связанных с использованием персональных данных и массовых данных, алгоритмической и системной предвзятостью, отсутствием прозрачности и проблемами надлежащей правовой процедуры, указывая на фундаментальную несовместимость между некоторыми видами использования алгоритмической полицейской технологии и конституционной защитой и защитой прав человека, особенно в отношении прав, связанных со свободой, равенством и неприкосновенностью частной жизни.

В части 5 («Международные последствия алгоритмической полицейской деятельности в области прав человека и Хартии прав человека») настоящий доклад применяет установленные правовые принципы в области прав человека и конституционного права к существующему или потенциальному использованию алгоритмических полицейских технологий в канадской системе уголовного правосудия, основываясь на результатах исследований, приведённых в части 4.

Части 1-3 настоящего доклада содержат справочный контекст, который закладывает основу для выводов и анализа исследований, изложенных в частях 4 и 5. В разделе 1.2 излагается методология, принятая авторами в ходе исследования и написания настоящего доклада. В части 2 («Социальный и исторический контекст») представлен социальный и исторический контекст, касающийся воздействия системной дискриминации в канадской системе уголовного правосудия, а также обзор того, каким образом системная предвзятость может проникать в полицейские данные. Именно эта системная дискриминация и систематические предубеждения лежат в основе многих вопросов прав человека, связанных с алгоритмической полицией. Часть 3 («Что такое алгоритмическая полиция?») содержит введение в алгоритмическую полицию, включая объяснение ее ключевых понятий и технологических

терминов, а также объяснение того, чем алгоритмическая полиция отличается от обычных методов полиции и наблюдения.

Методология

В настоящем докладе используется смешанный методический подход для изучения использования алгоритмических полицейских технологий в Канаде и способов, с помощью которых такие технологии могут поднимать вопросы прав человека и Хартии. Два основных этапа исследования для настоящего доклада - как алгоритмические полицейские технологии используются канадскими полицейскими службами (Часть 4) и оценка существующих или будущих алгоритмических полицейских технологий в области прав человека и конституционного права (Часть 5) – часто основывались на дискретных наборах методов. В целом эти этапы основывались на кабинетных исследованиях, правовых и политических исследованиях, подаче запросов о доступе к информации и свободе информации (FOI), неофициальных консультациях с экспертами по предметам, официальных исследовательских интервью с различными заинтересованными сторонами, экспертами и многодисциплинарном однодневном симпозиуме, включавшем совместные семинары. В настоящем докладе используется междисциплинарный и критический межсекторальный подход, объединяющий права человека, уголовное право, конституционное право, технологическое право и политику, научно-технические исследования и литературу по социальным наукам. Интеграция этих междисциплинарных и межсекторальных перспектив позволяет оценить потенциальные последствия для уязвимых сообществ, которые могут быть особенно затронуты использованием алгоритмических методов полицейской деятельности.

В оставшейся части этого раздела более подробно описываются методы исследования и анализа.

Сбор данных

Кабинетные исследования опирались на первичные и вторичные источники. Первичные источники включали документы правительственных и полицейских ведомств, которые были общедоступны в интернете, такие как отчёты совета полицейской службы, протоколы заседаний, уведомления о закупках, слайды презентаций и записи прошлых запросов других сторон о доступе к информации и свободе информации.

Вторичные источники включали освещение в средствах массовой информации алгоритмических полицейских технологий и связанных с ними инициатив, а также многочисленные юридические, политические, следственные и исследовательские доклады по различным аспектам алгоритмов, ИИ, уголовного правосудия и прав человека.

Эти доклады были подготовлены правительственными органами, неправительственными организациями, профессиональными ассоциациями (например, юридическими обществами или юридическими фондами), научно-исследовательскими учреждениями и правозащитными группами в Канаде и аналогичных юрисдикциях, таких как Соединённые Штаты, Соединённое Королевство и Европейский Союз.

Запросы о доступе к информации и свободе информации («запросы FOI»)740 были направлены в различные федеральные, провинциальные и муниципальные органы. Все эти органы были непосредственно связаны с правоохранительными функциями в канадской системе правосудия741. Процент ответов на эти запросы был различным.

В приложении A приводится копия текста шаблона, используемого для всех первоначальных запросов FOI. Практически в каждом запросе, в результате проводимых переговоров с указанием FOI сотрудника или аналитик. Такие сотрудники или аналитики регулярно стремились сузить круг запросов, уточнить тип записей, которые запрашивали авторы, или получить - часто непомерные - гонорары за обработку запроса. Для рассмотрения этих ответов, где это было возможно, были проведены последующие переговоры. На несколько запросов были получены ответы, подтверждающие привилегии в отношении запрашиваемых записей. Получение записей также требовало многочисленных последующих электронных писем и телефонных звонков, а для выполнения запросов требовалось значительное продление времени.

В некоторых случаях недопонимание приводило к преждевременному закрытию дел, в то время как в других случаях авторы должны были бы подать заявление об отказе от уплаты пошлин или обжаловать неудовлетворительные ответы в соответствующем регулирующем органе. После таких переговоров и

---

[740] Федеральные запросы информации по общественности регулируются Законом о доступе к информации RSC 1985 cA-1, в то время как запросы от провинций и муниципалитетов регулируются некоторым вариантом Закона о свободе информации и защите конфиденциальности. Для удобства обе формы запросов называются запросами FOI.

[741] Другие государственные учреждения, которым поручены другие государственные функции или обеспечение соблюдения других законов в Канаде, которые могут обращаться в органы уголовного правопорядка, выходят за рамки настоящего доклада, поскольку такие учреждения имеют иной круг общественных интересов и законодательных контекстов, чем учреждения, занимающиеся системой уголовного правосудия. К ним относятся органы контрразведки и национальной безопасности, целый ряд регулирующих органов, таких, как Канадское налоговое агентство и финансовые регулирующие органы, а также другие следственные органы, которым поручено расследовать преступления, не связанные с уголовными преступлениями в провинциях.

уплаты некоторых из более мелких сборов авторы получили отчёты по различным юрисдикциям и уровням государственного управления. Ответы на эти просьбы были включены в доклад, где это уместно[742].

Авторы провели восемь официальных исследовательских интервью (включая одно совместное интервью) для этого проекта в формате полуструктурированных интервью с участием в общей сложности девяти человек: пяти практикующих юристов, правозащитников, поставщиков общественных услуг и/или защитников расовой справедливости и четырех представителей правоохранительных органов по всей Канаде. Все исследовательские интервью проводились в соответствии с протоколом исследования, утверждённым Советом по этике исследований Университета Торонто. Ответы и выводы, полученные в ходе этих интервью, были включены в отчёт вместе с опрошенным лицом, идентифицированным или названным псевдонимом в соответствии с его согласием и принятым протоколом исследовательской этики.

Сбор данных с помощью исследовательских интервью ограничивался опросом профессионалов и признанных экспертов в соответствии с протоколом исследовательской этики проекта, поскольку авторы не были в состоянии ответственно участвовать в полном, передовом процессе консультаций сообщества с уязвимыми лицами. Однако адвокаты, защитники прав человека и расовой справедливости, а также члены общин, которые были опрошены, работают с ними, являются выходцами из своих соответствующих общин и интегрированы в них на повседневной основе. Кроме того, они знакомы и обладают опытом в отношении того, как система уголовного правосудия влияет и взаимодействует с обстоятельствами и опытом расовых и коренных народов и групп в Канаде.

Междисциплинарный симпозиум «автоматизированное принятие решений в системе уголовного правосудия» был совместно организован юридической комиссией Онтарио, лабораторией граждан и Ассоциацией адвокатов по уголовным делам 22 марта 2019 года. Симпозиум проходил по правилам Чатем-Хауса[743]. Этот симпозиум был закрытым мероприятием, которое способствовало откровенным междисциплинарным дискуссиям среди более чем 60 участников о проблемах, возникающих при использовании автоматизированных инструментов принятия решений на различных этапах

---

[742] Несколько запросов FOI, направленных для этого отчета в ноябре 2018 года, остаются невыполненными на момент написания.

[743] Справочные материалы симпозиума доступны по адресу: <https://www.lco-cdo.org/wp-content/uploads/2019/03/Background-Info- Package-1.pdf>. Правило Chatham House гласит, что "участники свободны в использовании полученной информации, но ни личность, ни принадлежность говорящего (говорящих), ни принадлежность любого другого участника не могут быть раскрыты". See Chatham House: The Royal Institute of International Affairs, «Chatham House Rule,» Accessed 10 August 2018, <https://www.chathamhouse.org/chatham-house-rule>.

системы уголовного правосудия, включая полицейскую деятельность, предварительное заключение, вынесение приговоров, оценку рисков и исправительные работы.

Участники были проинформированы и дали согласие на проведение дискуссий и семинаров, информирующих об исследованиях и публикациях, таких как настоящий доклад. Выводы, сделанные на симпозиуме, легли в основу некоторых анализов, приведённых в настоящем докладе.

Правовой анализ собранных данных

Права человека и правовой анализ в настоящем докладе опираются на международное право в области прав человека и Канадское право в области прав человека, уголовное и конституционное право. В настоящем докладе основное внимание уделяется судебной практике в соответствии с канадской Хартией прав и свобод. В то время как канадское конституционное право обеспечивает прочные рамки прав для отдельных лиц, которые регулируют использование полицейских следственных полномочий, новые технологии и их новое использование часто ставят правовые вопросы, которые ранее не были предметом Конституционного разбирательства. В результате в настоящем докладе также анализируются соответствующие международные обязательства Канады в области прав человека на том основании, что они служат основой для толкования прав, закрепленных в Хартии, а также обеспечивают параллельный правовой режим, который налагает обязательства в области прав человека на канадское правительство. Такие обязательства дополняют канадское законодательство в области прав человека.

Социально-исторический контекст

Настоящий доклад составлен в более широком контексте вопросов, связанных с системной предвзятостью и дискриминацией в обществе и в системе уголовного правосудия. В этом контексте необходимо использовать технологию алгоритмической полицейской деятельности, чтобы адекватно учитывать потенциальные последствия и риски этой технологии, особенно в том, что касается прав человека и конституционных прав. В разделе 2.1 приводится контекст, связанный с правительственными и судебными выводами, которые привлекают внимание к системной предвзятости и расизму в системе уголовного правосудия Канады, и рассматриваются последствия

системной дискриминации для отдельных лиц и общин. В разделе 2.2 дается обзор того, каким образом систематическая предвзятость может проникать в данные полиции. Для отдельных лиц и общин, затронутых системой уголовного правосудия в Канаде, неблагоприятные последствия могут быть значительными и длительными. Если систематические предубеждения пронизывают наборы данных, которые производятся в канадской системе уголовного правосудия, эти предубеждения могут быть внедрены и увековечены алгоритмическими полицейскими технологиями в ущерб отдельным лицам и общинам, которые были предметом исторической дискриминации.

Уголовное правосудие и системная дискриминация в Канаде

Существование систематических предубеждений и расизма в системе уголовного правосудия хорошо признано в Канаде и привело к непропорциональному воздействию на чернокожие, коренные, малообеспеченные, ЛГБТ, расовые и другие маргинализированные общины. Действующие лица системы правосудия, исследователи, журналисты-расследователи, правительственные органы и органы по правам человека задокументировали и привлекли внимание к чрезмерному надзору за полицией и чрезмерному тюремному заключению чернокожих и коренных жителей в канадской системе уголовного правосудия[744].

Чрезмерная полицейская деятельность включает в себя непропорциональный контроль со стороны правоохранительных органов за расовыми и коренными лицами в обстоятельствах, когда эти лица не совершают никаких противоправных действий и подвергаются более жесткому обращению со стороны правоохранительных органов. Например, исследования показывают, что лица с расовой принадлежностью чаще подвергаются аресту за мелкие правонарушения, чем лица без расовой принадлежности, что приводит к чрезмерно суровому обращению за правонарушения, не связанные с соображениями общественной безопасности[745]. Другие данные показывают, что, несмотря на сходное употребление каннабиса в различных расовых группах, чернокожие и коренные жители чрезмерно представлены при арестах за хранение каннабиса в Канаде и с большей вероятностью будут содержаться под стражей и доставлены в суд под залог, а не освобождены из полицейского участка[746]. Такое чрезмерное патрулирование имеет тревожные последствия и

---

[744] Там же

[745] Там же

[746] Rachel Browne, «Black and Indigenous people are overrepresented in Canada's weed arrests» (18 April 2018) Vice <https://www.vice.com/en_ca/article/d35eyq/black-and-indigenous-people-are-overrepresented-in-canadas-weed-

последствия, включая непропорциональное задержание, допрос и обыск лиц, принадлежащих к расе. Хотя такая деятельность может привести к обнаружению нескольких лиц с незаконными веществами или другой контрабандой – как это было бы в случае, если бы нерасистские лица были непропорционально остановлены и обысканы – она также часто неоправданно и несправедливо нацелена на подавляющее большинство, которые не делают ничего плохого, и эта практика порождает предвзятые статистические данные о целевых группах.

Верховный Суд Канады признал чрезмерную представленность коренных народов во всех аспектах уголовного судопроизводства как «кризис в канадской системе уголовного правосудия ... [это] вскрывает печальную и насущную социальную проблему».747 «Участники системы правосудия и законодатели продолжают бороться и якобы работают над устранением последствий этого исторического и продолжающегося наследия. По состоянию на январь 2020 года коренные жители составляли всего 5% населения Канады, в то время как сейчас, впервые в истории, они превышают 30% от общей численности населения, находящегося под федеральной опекой.748 Как цитирует Верховный Суд Канады, профессор Майкл Джексон писал, что «в историческом контексте тюрьма стала для многих молодых коренных жителей современным эквивалентом того, что представляла собой индийская школа-интернат для их родителей.»749 В заключительном докладе канадской комиссии по установлению истины и примирению содержится призыв ко всем уровням правительства заняться проблемой крайне непропорционального тюремного заключения коренных народов, которое продолжает расти.750

Исследователи и судебные расследования также привлекают внимание к чрезмерному полицейскому надзору и расовому профилированию расистски настроенных лиц, особенно членов чернокожих и коренных общин.[751] В

---

arrests>; Jim Rankin & Sandro Contenta, «Toronto marijuana arrests reveal 'startling' racial divide», Toronto Star (6 July 2017), <https://www.thestar.com/news/insight/2017/07/06/ toronto-marijuana-arrests-reveal-startling-racial-divide.html>; Alex Luscombe and Akwasi Owusu-Bempah, «Why legalization won't change racial disparities in cannabis arrests», VICE (19 April 2018), <https://www.vice.com/en_ca/article/gymnym/why-legalization-wont-change-racial- disparities-in-cannabis-arrests>.

747 R v Gladue, [1999] 1 SCR 688 at para 64.

748 Government of Canada, Office of the Correctional Investigator, «Indigenous People in Federal Custody Surpasses 30%: Correctional Investigator Issues Statement and Challenge», News Release (21 January 2020), <https://www.oci-bec.gc.ca/cnt/comm/press/press20200121- eng.aspx>.

749 R v Gladue, [1999] 1 SCR 688 at para 60.

750 Комиссия по установлению истины и примирению Канады, почитанию истины, примирения во имя будущего: резюме заключительного доклада Комиссии по установлению истины и примирению Канады (December 2015) <http://nctr.ca/assets/reports/Final%20Reports/Executive_Summary_English_Web. pdf>.

751 See generally, David Tanovich, The Colour of Justice (Toronto: Irwin Law, 2006); Ontario Human Rights Commission, Under Suspicion: Research and consultation report on racial profiling in Ontario (April 2017) <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation- report-racial-profiling-ontario>; Ontario Human Rights Commission, A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service (November 2018) <http://www.ohrc.on.ca/en/public-interest-inquiry-racial- profiling-and-discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-

докладе независимого обзора уличных проверок за 2018 год судья Майкл Х. Таллох обнаружил, что данные полицейских служб по всему Онтарио свидетельствуют о непропорциональном количестве полицейских остановок и задержаний с участием коренных, чернокожих и других расовых общин, а также молодёжи и людей из обездоленных социально-экономических групп.[752] При задержании людей на улице полиция имеет противоречивую и давно осуждаемую[753] практику регулярного запроса у людей идентификационной информации, которая затем записывается в полицейские базы данных наряду с другой информацией, полученной в результате встречи: о местонахождении человека, его деятельности и социальных ассоциациях, местоположение, деятельность и социальные связи индивида.[754]

Данные о непропорциональном полицейском надзоре за расовыми общинами и расовом профилировании всплыли по всей Канаде, в том числе в Монреале,[755] Галифаксе,[756] Эдмонтоне,[757] Калгари[758] и Ванкувере.[759] Газета «Торонто Стар» сообщила, что с 2008 по середину 2011 года «число молодых чернокожих и коричневых мужчин в возрасте от 15 до 24 лет, зарегистрированных в каждой из 72 патрульных зон города, превышает

---

and-racial-discrimination-black>; LogicalOutcomes, «'This Issue Has Been with Us for Ages': A Community-Based Assessment of Police Contact Carding in 31 Division» (November 2014).

[752] The Honourable Michael H. Tulloch, Report of the Independent Street Checks Review (2018) at page 44 <https://www.mcscs.jus.gov.on.ca/ sites/default/files/content/mcscs/docs/StreetChecks.pdf>

[753] «Ontario report finds carding has little to no value for law enforcement, should be sharply curtailed», The Globe and Mail (2 January 2019), <https://www.theglobeandmail.com/canada/article-ontario-report-finds-little-to-no-evidence-that-controversial-practice/>; The Honourable Michael H. Tulloch, Report of the Independent Street Checks Review (2018) at page 44 <https://www.mcscs.jus.gov.on.ca/sites/default/files/content/ mcscs/docs/StreetChecks.pdf>; Ontario Human Rights Commission, «Policy on eliminating racial profiling in law enforcement» at 4.2.6.2, <http:// www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>; Scot Wortley, Halifax, Nova Scotia: Street Checks Report (March 2019) <https://humanrights.novascotia.ca/streetchecks>.

[754] Идентификационная информация также, как правило, используется для проведения обысков в рамках КПИК, касающихся лица, с которым сталкивается полиция. Обыск в КПИК рассматривается как обыск в соответствии с разделом 8 Канадской хартии прав и свобод, раздел 7, часть I, Конституционного закона 1982 года, который включен в приложение к Канадскому закону 1982 года (Соединенное Королевство), 1982 год, с 11, s 8; R v Walters, 2018 ONSC 4194, в п. 125. Таким образом, члены расовых, малообеспеченных или иным образом перегруженных полицией общин, которые в непропорционально большой степени подвергаются этой практике, могут быть занесены в базы данных полиции без совершения каких-либо противоправных действий, и их личная информация впоследствии может быть получена правоохранительными органами и другими федеральными ведомствами Канады или даже в некоторых случаях правоохранительными органами Соединенных Штатов. Graeme Norton, Presumption of Guilt? The Disclosure of Non¬Conviction Records in Police Background Checks, Canadian Civil Liberties Association (May 2012) <https://ccla.org/cclanewsite/wp-content/ uploads/2015/02/Presumption-of-Guilt.pdf> at 7.

[755] Toula Drimonis, «Racial profiling a systemic problem for Montreal police», National Observer (24 April 2018), <https://www.nationalobserver. com/2018/04/24/opinion/racial-profiling-systemic-problem-montreal-police>.

[756] Scot Wortley, Halifax, Nova Scotia: Street Checks Report (March 2019) <https://humanrights.novascotia.ca/streetchecks>.

[757] Andrea Huncar, «Indigenous women nearly 10 times more likely to be street checked by Edmonton police, new data shows», CBC News (27 June 2017), <https://www.cbc.ca/news/canada/edmonton/street-checks-edmonton-police-aboriginal-black-carding-1.4178843>.

[758] Rocky Mountain Civil Liberties Association, «Calgary Police data suggests Police Carding is Greatest in Diverse Neighbourhoods» (9 May 2016), <http://www.rmcla.ca/blog/?p=394>.

[759] Globe and Mail, «Vancouver Police Department's use of carding disproportionately targets Indigenous people» (4 June 2018), <https://www. theglobeandmail.com/canada/british-columbia/article-vancouver-police-departments-use-of-carding-disproportionately/>.

фактическое число цветных молодых людей, проживающих в этих районах.[760] «Столкновения гражданских лиц с полицией на улице - это лишь один пример полицейских методов, которые непропорционально сильно влияют на расовые и маргинальные общины. В докладах также освещаются другие формы государственного надзора, нацеленного на расовые, маргинальные и политические сообщества.[761]

Для отдельных лиц и общин, на которые оказывает влияние система правосудия в Канаде, неблагоприятные последствия: подвергаются повышенному полицейскому контролю, судебным разбирательствам и длительному тюремному заключению.

Последствия включают повышенный уровень рецидивизма[762] а также негативные последствия для здоровья, бедности и человеческого достоинства,[763] и возобновление циклов нищеты и угнетения, которые оставляют людей уязвимыми и в обстоятельствах, которые могут привести к дальнейшему полицейскому контролю. Даже осуждение, не связанное с лишением свободы, и судимость могут иметь пожизненные последствия, включая стигматизацию, значительные неблагоприятные последствия для перспектив трудоустройства или карьеры, иммиграционные последствия и

---

[760] Jim Rankin & Patty Winsa, «Known to police: Toronto police stop and document black and brown people far more than whites», The Toronto Star (9 March 2012) <https://www.thestar.com/news/insight/2012/03/09/known_to_police_toronto_police_stop_and_document_black_and_brown_ people_far_more_than_whites.html?li_source=LI&li_medium=star_web_ymbii>.

[761] Reg Whitaker, Gregory S. Kealey & Andrew Parnaby, Secret Service: Political Policing in Canada From the Fenians to Fortress America (Toronto: University of Toronto Press, Scholarly Publishing Division, 2012). For example, numerous reports of targeting of Muslim individuals in Canada
have been uncovered. See Colton Praill, «Muslim students in Saskatchewan receiving calls from CSIS, say university students», Global News (20 November 2018) <https://globalnews.ca/news/4683333/muslim-students-saskatchewan-calls-csis/>; Benjamin Shiller, «Activists launch 'don't talk' campaign to denounce CSIS 'intimidation tactics'«, The Toronto Star (30 January 2012), <https://www.thestar.com/news/canada/2012/01/30/
activists_launch_dont_talk_campaign_to_denounce_csis_intimidation_tactics.html>. The RCMP have also been reported to target Indigenous rights activists: see Andrew Nikiforuk, «When Indigenous Assert Rights, Canada Sends Militarized Police», The Tyee (17 January 2019), <https:// thetyee.ca/Analysis/2019/01/17/Indigenous-Rights-Canada-Militarized-Police/>; Miles Howe & Jeffrey Monaghan, «Strategic Incapacitation of Indigenous Dissent: Crowd Theories, Risk Management, and Settler Colonial Policing» (2018) 43:4 Canadian Journal of Sociology 325, <https://journals.library.ualberta.ca/cjs/index.php/CJS/article/view/29397/21432?fbclid = IwAR0gOWPQ6ZE6Om8Tq4u0vO1rF2ndSSfvbtjLOeM4U_B2F_ YzYeqRNuipHQw>; «Snooping on First Nations activist went too far, privacy commissioner says», CBC News (29 May 2013), <https://www.cbc.ca/news/canada/snooping-on-first-nations-activist-went-too-far-privacy-commissioner-says-1.1364426>. In 2017, investigative reporting by the Toronto Star also brought to light the RCMP's controversial use of a racial profiling screening tool at a border crossing between the United States
and Canada. This practice reportedly ended a controversial practice that was reportedly brought to an end after it was brought to the public's attention: Michelle Shephard, «RCMP will redact more than 5,000 records collected using questionnaire targeting Muslim asylum seekers», The Toronto Star (27 November 2017) <https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected- using-questionnaire-targeting-muslim-asylum-seekers.html>.

[762] Paula Smith, Claire Goggin, & Paul Gendreau, «The Effects of Prison Sentences and Intermediate Sanctions on Recidivism: General Effects and Individual Differences» (January 2002), <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ffcts-prsn-sntncs/index-en.aspx>.

[763] Fiona Kouyoumdijian et al., «Health status of prisoners in Canada» (March 2016) 62 Clinical Review 215 <https://www.cfp.ca/content/ cfp/62/3/215.full.pdf>.

ограничение поездок. Доверие к алгоритмическим прогнозам, использующим эти завышенные показатели рецидивизма, вероятно, усугубит существующие предубеждения.

Неблагоприятные последствия также очевидны при рассмотрении воздействия полицейских остановок и задержаний на отдельных лиц (а также их общины и семьи), которые являются объектом постоянного контроля.[764]

Верховный Суд Канады недавно заявил, что непропорциональное полицейское преследование расовых меньшинств посредством кардинга «наносит ущерб физическому и психическому здоровью человека» и «влияет на его способность добиваться трудоустройства и получения образования».[765] Суд постановил что «эта практика способствует продолжающейся социальной изоляции расовых меньшинств, способствует утрате доверия к справедливости нашей системы уголовного правосудия и увековечивает криминализацию».[766]

Длительное социальное и психологическое воздействие на лиц, которые были вовлечены в систему уголовного правосудия или подвергались ей в качестве подозреваемых или обвиняемых, усиливает важность обеспечения того, чтобы алгоритмические методы полицейской деятельности не подвергали людей риску потенциальных ложных срабатываний (например, ошибки, которая неверно идентифицирует человека или чрезмерно представляет воспринимаемый им риск для общества) или скрытой дискриминации, которая может привести к предвзятым арестам, задержаниям или тюрьмам.

Предвзятость и неточности в полицейских данных

Технологии алгоритмического контроля[767] обычно зависят от обработки больших объёмов данных из широкого набора источников. Эти данные используются для обучения алгоритмов или в качестве входных данных для

---

[764] Scot Wortley & Akwasi Owusu-Bempah, «The Usual Suspects: Police Stop and Search Practices in Canada» (2011) 21 Policing and Society 395 at 400-401, https://www.researchgate.net/publication/238046161_The_Usual_Suspects_Police_Stop_and_Search_Practices_in_Canada>; see also: Sophie de Saussure, «Parents in prison: A public policy blind spot», Policy Options (12 July 2018), <https://policyoptions.irpp.org/ magazines/may-2018/parents-in-prison-a-public-policy-blind-spot/>.

[765] R v Le, 2019 SCC 34 at para 95.

[766] R v Le, 2019 SCC 34 at paras 93-95 [citations omitted]. See also: The Honourable Roy McMurtry, Review of the Roots of Youth Violence, Volume 1 (2008) at 77-78, <http://www.children.gov.on.ca/htdocs/english/documents/youthandthelaw/rootsofyouthviolence-vol1.pdf>; Scot Wortley & Akwasi Owusu-Bempah, «The Usual Suspects: Police Stop and Search Practices in Canada» (2011) 21 Policing and Society 395 at 400-401, <https://www.researchgate.net/publication/238046161_The_Usual_Suspects_Police_Stop_and_Search_Practices_in_Canada>.

[767] Алгоритмические технологии контроля будут более подробно определены и внедрены в части 3 («What is 'Algorithmic Policing'?»).

формирования прогнозов о людях или местах, прогнозов, на которые затем действуют правоохранительные органы. Источники данных могут включать статистику криминальных опросов, сообщения в социальных сетях, данные геолокации, журналы вызовов кризисного центра, данные о травмах в больницах или данные о преступной деятельности, собранные не полицейскими сотрудниками Службы безопасности, такими как полицейскими транзита, кампуса или торгового центра, а также частной охраной.[768]

Для целей настоящего доклада под полицейскими данными понимаются статистические и биографические данные, которые собираются и регистрируются полицейскими службами (например, данные о задержаниях и сообщённых преступлениях), а также данные, которые могут составлять часть судимости лица (например, аресты, обвинительные приговоры).[769] Многие источники полицейских данных могут не быть объективными или точными показателями преступной деятельности, но эти данные регистрируются в муниципальных, провинциальных и федеральных полицейских базах данных, которые, в свою очередь, влияют на будущие взаимодействия между пострадавшим лицом и полицией или системой уголовного правосудия. Везде, где в настоящем докладе говорится об алгоритмической обработке данных из полицейских баз данных, такие наборы данных называются историческими массовыми полицейскими данными или историческими полицейскими наборами данных. Эти термины используются для того, чтобы подчеркнуть «большую информационную» природу алгоритмической полиции и сосредоточиться на обстоятельствах, когда большие объёмы уже существующих полицейских данных используются для обучения полицейских алгоритмов или иным образом массово обрабатываются такими алгоритмами.

Исторические массовые полицейские данные следует отличать от фрагментарных данных, обрабатываемых на индивидуальной основе, например, с использованием письменных заметок сотрудника полиции в случае конкретного человека (в отличие от оцифровки всех письменных заметок каждого сотрудника и подачи этого набора данных в алгоритм).

В этом разделе кратко рассматриваются некоторые ключевые проблемы с различными типами полицейских данных, которые могут быть использованы

---

[768] С благодарностью Терезе Скассе за то, что она указала на это. Конкретные типы алгоритмических технологий и источников данных более подробно рассматриваются в части 4. («Algorithmic Policing in Canada: The Current Landscape»).

[769] Для удобства использования во всем докладе термин "данные полиции" будут использоваться в качестве общего термина для описания этих классов широких данных, доступных для полиции и хранящихся в полицейских базах данных. На некоторые аспекты данных, такие, как обвинительные приговоры по уголовным делам, влияет то, что происходит на более поздних стадиях уголовного судопроизводства в уголовных судах, но на данные, тем не менее, существенно влияет деятельность правоохранительных органов (например, в качестве правоохранительных органов выбирает, какие дела передавать в суд на основании решений о предъявлении обвинений), и то, что ведётся правоохранительными органами в базах данных.

алгоритмами или для получения автоматизированного решения уголовного правосудия в отношении отдельного лица.

Использование данных, собранных в ходе полицейских остановок, создаёт особую проблему в свете давних и широко распространённых сообщений о дискриминационной практике и стереотипах по всей Канаде.

Отчёт 2019 года об уличных проверках в Галифаксе показал, что полиция в шесть раз чаще нацеливается на чернокожих людей, чем на белых.[770]В Онтарио, как уже давно сообщалось, полицейские остановки и остановки движения непропорционально сильно затрагивают чернокожих, коренных и других расовых индивидуумов.[771] Хотя спорная практика «прочёсывания» попала под некоторые ограниченные правила в Онтарио в 2017 году[772] данные «прочёсывания», собранные до 2017 года, все ещё доступны полицейским службам в Онтарио, и доступ лишь частично ограничен в отношении некоторых данных «прочёсывания», собранных с 2017 года.[773] Многие полицейские службы также не соблюдают требования прозрачности отчётности о практике остановки полиции, которые требуются в соответствии с регламентом.[774] Данные, полученные полицейскими службами по всей стране, выявили сходные закономерности, при которых чернокожие и коренные народы чрезмерно представлены в полицейских данных.[775]

В результате полиция получает доступ к несоразмерно большому количеству информации о расовых и коренных народах, а также о некоторых районах, которые затем могут быть использованы в полицейских алгоритмах.

Базы данных банд: членство в банде или ассоциация с членами банд часто рассматривается правоохранительными органами как фактор риска, и

---

[770] Scot Wortley, Halifax, Nova Scotia: Street Checks Report (March 2019) at 105 <https://humanrights.novascotia.ca/streetchecks>.

[771] See The Honourable Michael H. Tulloch, Report of the Independent Street Checks Review (2018) at 44 <https://www.mcscs.jus.gov.on.ca/ sites/default/files/content/mcscs/docs/StreetChecks.pdf>.

[772] В докладе Независимого обзора проверок улиц судья Туллоха определяет "проверку улиц" как любое происшествие, когда "сотрудник полиции получает информацию, касающуюся какого-либо лица, за пределами полицейского участка, который не является частью расследования "Кардинг", относится к подгруппе уличных проверок ", в которых сотрудник полиции случайным образом просит лицо предоставить идентифицирующую информацию, когда это лицо не подозревается в совершении какого-либо преступления, нет также никаких оснований полагать, что данное лицо располагает информацией о каком-либо преступлении. "Ibid at 2.

[773] Ibid at 143; Collection of Identifying Information in Certain Circumstances - Prohibition and Duties, O. Reg. 58/16, s 2 and 9.

[774] Danielle, McNabb, Dennis Baker & Troy Riddell, «Mandatory police carding data severely lacking across Ontario», Toronto Star (14 August 2019), <https://www.thestar.com/opinion/contributors/2019/08/14/mandatory-police-carding-data-severely-lacking-across-ontario.html>.

[775] Sunny Dhillon, «Vancouver Police Department's use of carding disproportionately targets Indigenous people», The Globe and Mail (4 June 2018) <https://www.theglobeandmail.com/canada/british-columbia/article-vancouver-police-departments-use-of-carding-disproportionately/>; Rocky Mountain Civil Liberties Association, «Calgary Police data suggests Police Carding is Greatest in Diverse Neighbourhoods» (9 May 2016), <http://www.rmcla.ca/blog/?p=394>; Andrea Huncar, «Indigenous women nearly 10 times more likely to be street checked by Edmonton police, new data shows», CBC News (27 June 2017) <https://www.cbc.ca/news/canada/edmonton/street-checks-edmonton-police-aboriginal-black- carding-1.4178843>.

информация, хранящаяся в «базах данных банд», может быть использована для информирования алгоритмической полицейской технологии.[776] Использование информации об объединении банд вызывает серьёзную озабоченность по поводу точности, поскольку определение правоохранительными органами причастности банд часто может быть проблематичным.[777] Например, в Суррее, Британская Колумбия, программа, в рамках которой полиция и школьный персонал совместно выявляли учащихся, подвергающихся риску бандитской деятельности, изучала такие факторы, как «одно- или многоэтническая» группа сверстников учащихся, «склонность к насилию и «общение с неподходящими людьми».[778]

По словам исследования общественной организации Торонто, занимающейся сокращением преступности, молодые люди регулярно вносятся в полицейские базы данных как члены банды, основанные на непроверенной информации или неверных предположениях школьного персонала, местных поставщиков услуг или сотрудников полиции.[779] Доктор Скотт Уортли, профессор криминологии из Университета Торонто, высказал озабоченность по поводу расплывчатости, неточности и манипулируемости критериев членов банд, используемых канадскими полицейскими службами.

Он также отметил, что пометка «бандитская ассоциация «может привести к тому, что законопослушные друзья и члены семьи будут классифицированы как «вовлечённые в банду».[780]

---

[776] For example, the Los Angeles Police Department considered gang membership in its person-focused predictive policing strategy known as the Chronic Offender Bulletin. See Issie Lapowsky, «How the LAPD Uses Data to Predict Crime», Wired (22 May 2018) <https://www.wired.com/ story/los-angeles-police-department-predictive-policing/>.

[777] Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 58; Scot Wortley, «Identifying Street Gangs: Definitional Dilemmas and Their Policy Implications» (2010), <http://publications.gc.ca/collections/ collection_2012/sp-ps/PS4-115-2011-eng.pdf>.

[778] Nathan Munn, «This B.C. city is tackling gang violence by profiling high school students», Vice (7 January 2019) <https://www.vice.com/ en_ca/article/59vv8x/this-bc-city-is-tackling-gang-violence-by-profiling-high-school-students>; Similarly, in the United States, researchers who claimed to develop an algorithm that identified gang members based on their Twitter posts—in particular, based on their use of «tough talk», certain words and emojis, and links to rap music videos—were criticized for the potentially discriminatory assumptions underlying the tool: Jordan Pearson, «Researchers Claim AI Can Identify Gang Members on Twitter», Vice (1 November 2016), <https://www.vice.com/en_us/article/ mg7kgx/researchers-claim-ai-can-identify-gang-members-on-twitter>.

[779] «Как тот, кто оценивает бандитские программы, многие дети помечены как вовлеченные или в банду, у директора школы, и даже когда дети не называют себя бандой, они помечены как банда, потому что они украли деньги на обед. Существует больше внешнего наложения этикеток. Затем это подается в другие агентства с небольшой достоверностью, в отличие от того, что на самом деле это школа, подтвердила местная служба". Интервью исследователя из Торонто, поставщика общественных услуг, занимающегося вопросами уголовного правосудия, Иоланда Сон и Синтия Кхоо (8 May 2019).

[780] Scot Wortley, «Identifying Street Gangs: Definitional Dilemmas and Their Policy Implications» (2010) at 13, <http://publications.gc.ca/ collections/collection_2012/sp-ps/PS4-115-2011-eng.pdf>. Кроме того, обзор базы данных о бандах Департамента полиции Чикаго за 2019 год показал, что Департамент не смог подтвердить точность обозначений своих банд, в том числе вопросы качества данных и транспарентности. Sanjana Karanth, «Inspector General Finds Chicago Gang Database Outdated, Inaccurate and Damaging», Huffington Post (11 April 2019) <https://www. huff ingtonpost.ca/entry/chicago-inspector-general-police-gang-database_n_5cafd2b2e4b082aab0831bf7>.

Дети могут быть не в банде, а связаны с бандой, потому что они бездомны или болтаются с ними из-за потребности в динамичном образе жизни. Полицейский сказал бы: «да, этот парень был в банде», потому что они связаны [...] Но это может быть просто бездомный ребенок, имеющий проблемы с наркотиками.

– Исследователь в компании, предоставляющей общественные услуги в Торонто.[781]

Сообщения представителей общественности: некоторые полицейские службы могут полагаться на сообщения о преступлениях, инициированные представителями общественности, для решения проблем, связанных с данными, полученными полицией.[782] Достоверность сообщений общественности как источника данных вызывает сомнения, как показано в докладе статистического управления Канады, указывающем, что «в 2014 году полиция никогда не обращала внимания на случаи виктимизации, как насильственные, так и ненасильственные. Чуть менее трети (31%) сообщили в полицию либо непосредственно пострадавшему (21%), либо каким-либо иным образом (10%)».[783]

Даже о таких имущественных преступлениях, как кражи со взломом и кражи автомобилей, полиции сообщают лишь в половине случаев.[784] Эти большие пробелы в сообщениях о преступлениях, генерируемых общественностью, могут существенно подорвать точность любых прогнозов преступности, которые зависят от этого источника данных.

Заниженные сведения о преступлениях: Некоторые расовые общины менее склонны сообщать о преступлениях из-за ранее существовавшей напряженности, языковых или культурных барьеров, страха быть депортированными, страха перед правоохранительными органами, предшествующего плохого опыта работы с полицией или недоверия к полицейским учреждениям из-за дискриминационной практики и истории. [785]

---

[781] Интервью исследователя из Торонто, поставщика общественных услуг, занимающегося вопросами уголовного правосудия, Иоланда Сон и Синтия Кхоо (8 May 2019).

[782] См., например, полицейское управление Ванкувера, использующее в своем алгоритме прогнозирования полиции только сообщения об имущественных преступлениях, подготовленные общественностью, о чем говорится в разделе 4.1 («Location-Focused Algorithmic Policing»).

[783] Samuel Perreault, «Criminal victimization in Canada, 2014» (23 November 2015) Juristat Catalogue no. 85-002-X at 23 <https://www150. statcan.gc.ca/n1/en/pub/85-002-x/2015001/article/14241-eng.pdf?st=RDyLQpoX>.

[784] Ibid at 25. См. также критику Терезы Скасса в отношении достоверности данных о публичных звонках: "Человек, который сообщает о краже из своего автомобиля, может через несколько дней понять, что предмет, который он должен был украсть, был просто утерян. Просто то, что о чем-то сообщают в полицию, не означает, что произошло преступление. Если карты просто отражают данные вызова и не обновляются по мере получения дополнительной информации об инцидентах, это снижает надежность информации ". Teresa Scassa, «Police Service Crime Mapping as Civic Technology: A Critical Assessment» (2016) 5:3 International Journal of E-Planning Research 13 at 19.

[785] The Honourable Michael H. Tulloch, Report of the Independent Street Checks Review (2018) at 45-46 <https://www.mcscs.jus.gov.on.ca/ sites/default/files/content/mcscs/docs/StreetChecks.pdf>; Community Oriented

Трансгендерные лица и общины также не могут сообщать о преступлениях «в результате их собственного или общинного опыта виктимизации или дискриминации со стороны правоохранительных органов».[786]

Насилие в отношении женщин и сексуальное насилие также являются значительно заниженными преступлениями из-за страха стигматизации, повторной виктимизации со стороны правоохранительных органов и недоверия к тому, что дело жертвы будет рассматриваться серьёзно.[787] Таким образом, алгоритмы полицейской деятельности, призванные предсказать виктимизацию, могут отражать только обстоятельства демографических групп, которые с большей вероятностью сообщат о преступлениях в полицию.

Недокументированные преступления: преступления, о которых сообщается, но которые игнорируются, будь то в результате ошибки, неправильного обращения или дискриминационных предположений и стереотипов.[788] Например, сексуальное насилие является одним из самых недооцениваемых преступлений в Канаде[789] из-за карательных социальных и институциональных барьеров, которые препятствуют жертвам и выжившим выступать вперёд.[790]Несмотря на это, отчёт о расследовании 2017 года показал, что канадская полиция отклонила примерно 20% сообщений о сексуальном насилии как «беспочвенные и, следовательно, необоснованные».[791]

Policing Services & Vera Institute of Justice, «How to Serve Diverse Communities» (2016) Police Perspectives: Building Trust in a Diverse Nation, No. 2 at 6 <https://www.securitepublique.gc.ca/lbrr/archives/ cnmcs-plcng/cn96061923-eng.pdf>. Deportation fears may also be a contributing factor to under-reporting: Cecilia Benoit, «Issue Brief: Sexual Violence Against Women in Canada», commissioned by the Federal-Provincial-Territorial Senior Officials for the Status of Women (December 2015), <https://cfc-swc.gc.ca/svawc-vcsfc/index-en.html>.

[786] Community Oriented Policing Services & Vera Institute of Justice, «How to Serve Diverse Communities» (2016) Police Perspectives: Building Trust in a Diverse Nation, No. 2 at 27 <https://www.securitepublique.gc.ca/lbrr/archives/cnmcs-plcng/cn96061923-eng.pdf>.

[787] См., например, "[Неполная отчетность] может быть фактором для определенных видов преступлений (таких как, например, сексуальное насилие или насилие в семье) (Johnson, 2012) или для определенных типов жертв, которые могут стремиться свести к минимуму свои контакты с полицией (например, уличные причастные лица). Занижение информации может быть также проблемой в общинах, где есть недоверие к полиции или где есть страх возмездия за сообщение о преступлениях в полицию. " Teresa Scassa, «Police Service Crime Mapping as Civic Technology: A Critical Assessment» (2016) 5:3 International Journal of E-Planning Research 13 at 21.

[788] «Полиция не является ни пассивным сборщиком информации, ни выявителем каждого нарушения закона. Каждое действие - или отказ от действий - со стороны сотрудника полиции, и каждое аналогичное решение, принятое полицейским департаментом, также является решением о том, как и нужно ли генерировать данные... принятие решений полицией формирует саму реальность, которую мы воспринимаем о преступлении и нарушении закона. Мы знаем о преступлениях, на которые обращает внимание полиция. С другими мы часто этого не делаем.» In Elizabeth E Joh, «Feeding the Machine: Policing, Crime Data, & Algorithms» (2017) 26:2 William & Mary Bill of Rights Journal 287 at 289-90 (footnotes omitted).

[789] Shana Conroy & Adam Cotter, «Self-reported sexual assault in Canada, 2014» (11 July 2017) Juristat, Catalogue no. 85-002-X at 4 <https:// www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/14842-eng.pdf>.

[790] See generally Alana Prochuk, «We Are Here: Women's Experiences of the Barriers to Reporting Sexual Assault» (November 2018) West Coast LEAF <http://www.westcoastleaf.org/wp-content/uploads/2018/10/West-Coast-Leaf-dismantling-web-final.pdf>. According to one survey, in 2014, 83% of sexual assaults in Canada were not reported to police, while only 5% were: Department of Justice, «Just Facts: Sexual Assault» (May 2017) at 1 <https://www.justice.gc.ca/eng/rp-pr/jr/jf-pf/2017/may02.html>.

[791] Robyn Doolittle, «Why police dismiss 1 in 5 sexual assault claims as baseless» (3 February 2017) The Globe and Mail<https://www.theglobeandmail.com/news/investigations/unfounded-sexual-assault-canada-main/article33891309/>.

В рамках документированных преступлений может увеличиться разрыв между обвинительными приговорами за сексуальное насилие и фактической распространённостью сексуального насилия в Канаде – проблема, которая систематически наносит вред женщинам и девочкам и нарушает их права человека.[792] Использование таких данных для обучения полицейского алгоритма может неявно закрепить в модели предубеждения и предположения, которые приводят как к занижению отчётности, так и к чрезмерному отклонению преступлений сексуального насилия.

Аресты: хотя данные об арестах часто используются в алгоритмических полицейских технологиях,[793] аресты не являются фактологически или юридически точными репрезентациями преступной деятельности. Арестованные лица могут быть освобождены, с них могут быть сняты обвинения или в конечном итоге они могут быть оправданы. Хотя в Канаде существует относительно мало исследований по этому вопросу, особенно с учётом того, что власти не обязаны собирать или раскрывать данные о расе, некоторые данные и сообщения показывают, что лица, принадлежащие к расе и коренным народам, непропорционально чаще подвергаются аресту за преступления, связанные с хранением каннабиса (несмотря на аналогичные показатели употребления каннабиса среди населения в целом), или чрезмерно суровому обращению за мелкие правонарушения по сравнению с белыми лицами.[794] Кроме того, аресты за совершение преступлений, связанных с отправлением правосудия, которые составили более одного из пяти всех уголовных дел взрослых, завершённых в 2015-2016 годах,[795] могут оказать особое воздействие на маргинальные группы. К правонарушениям, связанным с препятствием правосудия, относятся неявка в суд, нарушение постановления об условно-досрочном освобождении, незаконное пребывание на свободе и невыполнение постановления. Некоторые из этих арестов являются результатом введения неоправданных или ненадлежащих условий, которые накладывают необоснованные ограничения на уязвимых лиц. Например, лица,

---

[792] Cristine Rotenberg, «From arrest to conviction: Court outcomes of police-reported sexual assaults in Canada, 2009 to 2014» (26 October 2017) Juristat, Catalogue no. 85-002-X, at 4, <https://www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/54870-eng.pdf>. Men and non¬binary individuals are also systematically unlikely to report instances of sexual assault.

[793] См., например, прогнозные стратегии охраны правопорядка в Чикаго, Новом Орлеане и Канзас-Сити, штат Миссури, как описано в книге Эндрю Фергюсона "Рост политики в отношении больших данных: наблюдение, гонка и будущее правоохранительных органов": Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 44-51.

[794] Rachel Browne, «Black and Indigenous people are overrepresented in Canada's weed arrests» (18 April 2018) Vice <https://www.vice.com/ en_ca/article/d35eyq/black-and-indigenous-people-are-overrepresented-in-canadas-weed-arrests>; Jim Rankin & Sandro Contenta, «Toronto marijuana arrests reveal 'startling' racial divide», Toronto Star (6 July 2017), <https://www.thestar.com/news/insight/2017/07/06/toronto-marijuana- arrests-reveal-startling-racial-divide.html>. Akwasi Owusu-Bempah, «Race, Crime, and Criminal Justice in Canada», in The Oxford Handbook of Ethnicity, Crime, and Immigration (Oxford: Oxford University Press, 2014) at 15 <https://www.researchgate.net/publication/274314275_Race_ Crime_and_Criminal_Justice_in_Canada>.

[795] Department of Justice, «The Canadian Criminal Justice System:OverallTrends and Key Pressure Points» (23 November 2017) <https://www.justice.gc.ca/eng/rp-pr/jr/press/>.

борющиеся с зависимостью, с большей вероятностью могут быть арестованы за нарушение условий освобождения под залог, которые требуют от них воздерживаться от наркотиков или алкоголя, в то время как лица, находящиеся в ненадёжном положении, могут подвергнуться аресту за нарушение условий освобождения под залог, которые требуют от них соблюдения комендантского часа или пребывания по фиксированному адресу.

Обвинительные приговоры и признание вины: в отличие от арестов, обвинительные приговоры юридически считаются доказательством того, что человек совершил преступление. Однако, данные об осуждении также ненадёжны по ряду причин. Как отмечалось выше, данные об осуждении также будут пронизаны последствиями систематической предвзятости и чрезмерной полицейской деятельности, поскольку обвинительные приговоры могут возникать только из дел, которые доводятся до суда правоохранительными органами. В дальнейшем, отдельные лица могут быть несправедливо осуждены.[796] Некоторые группы, такие как женщины и представители коренных народов, особенно уязвимы для неправомерных обвинений.[797] Множество обвинительных приговоров исходит из случаев, когда отдельные лица признали себя виновными и отказались от своего права на судебное разбирательство. Подавляющее большинство уголовных дел не идут в суд, а вместо этого рассматриваются через резолюции, в том числе резолюции о признании вины.[798] Следовательно, статистические данные о количестве осуждённых по уголовным делам в Канаде в основном состоят из обвинительных приговоров о признании вины, хотя «фактически невиновные люди в Канаде иногда , по целому ряду причин, признают себя виновными в преступлениях, которых не совершали».[799]

Невиновные лица, которым было отказано в освобождении под залог или которые полагают, что они вряд ли будут освобождены под залог, могут мотивированно признать себя виновными с целью получения более раннего освобождения из-под стражи.[800] В 2017 году исследователи Министерства

---

[796] Innocence Canada has been involved in the exonerations of 23 individuals since 1993: Innocence Canada, «Exonerations» <https://www. innocencecanada.com/exonerations/>. Неизвестно, сколько неправомерных приговоров остаются незамеченными; посмотрите федеральных/Провинциальных/Территориальных Глав Подкомиссии Судебного преследования по Предотвращению Неправомерных Убеждений, Невинность под угрозой: Потребность в Длительной Бдительности, чтобы предотвратить Неправомерные Убеждения в Канаде: The Need for Continued Vigilance to prevent Wrongful Convictions in Canada (2018) at 1 <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf>.

[797] Ibid at 221.

[798] Хотя в Канаде нет национальных статистических данных о признании вины, исследователи подсчитали, что приблизительно 90% уголовных дел решаются путем признания вины. See Angela Bressan & Kyle Coady, «Guilty pleas among Indigenous people in Canada» (2017) at 6 <http://publications.gc.ca/site/eng/9.851369/publication.html>.

[799] Федеральные/Провинциальные/Территориальные Главы Подкомиссии Судебного преследования по Предотвращению Неправомерных Убеждений, Невинность под угрозой: Потребность в Длительной Бдительности, чтобы предотвратить Неправомерные Убеждения в Канаде (2018), at 169 <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng. pdf>.

[800] Ibid at 179-180.

юстиции обнаружили, что коренные жители «иногда признают себя виновными, даже если они невиновны..., могут иметь обоснованную защиту или иметь основания поднимать вопросы Хартии. [801] Исследования также показали, что другие маргинальные группы, включая молодёжь, лица с когнитивными трудностями, лица, испытывающие психическое здоровье или аддикции проблемы, лица, живущие в нищете, и расистские индивиды также могут быть особенно подвержены риску ложного признание вины.[802] Отсутствие финансирования юридической помощи способствовало ложному признанию вины со стороны лиц, - находящихся в невыгодном соцтально-экономическом положении. [803] Проблема ложного признания вины дополнительно усугубляется непропорциональными отказами в освобождении под залог и канадская система правосудия не учитывает культурные представления коренных народов о правосудии, которые существено отличаются о того, как уголовное правосудие понимается и рассматривается в канадском законодательстве.[804]

Вышеизложенное не является исчерпывающим перечнем всех форм данных, которые могут определять, как работает алгоритм полицейской деятельности, и не все рассмотренные типы полицейских данных обязательно используются в качестве обучающих данных или входных данных для алгоритмов полицейской деятельности в Канаде.[805]Однако тот факт, что все наиболее распространённые источники полицейских данных затронуты проблемами, которые могут исказить надёжность этих источников, не должен вызвать серьёзные вопросы и опасения по поводу использования методов управления большими данными, таких как алгоритмическая полиция. Конкретные проблемы, связанные с неточностями и предвзятостью данных, обсуждаются на протяжении всего юридического анализа, представленного в

---

[801] Angela Bressan & Kyle Coady, «Guilty pleas among Indigenous people in Canada» (2017) at 9 <http://publications.gc.ca/site/eng/9.851369/ publication.html>.

[802] Ibid at 6.

[803] See, e.g., Dough Schmidt, «Windsor lawyers worry that funding cuts mean more jail for poor, vulnerable» (20 June 2019) Windsor Star, <https://windsorstar.com/news/local-news/windsor-lawyers-worry-that-funding-cuts-mean-more-jail-for-poor-vulnerable>.

[804] Angela Bressan & Kyle Coady, «Guilty pleas among Indigenous people in Canada» (2017) at 6 <http://publications.gc.ca/site/eng/9.851369/ publication.html>; Abby Deshman & Nicole Myers, «Set Up to Fail: Bail and the Revolving Door of Pre-trial Detention», Canadian Civil Liberties Association and Education Trust (July 2014), <https://ccla.org/cclanewsite/wp-content/uploads/2015/02/Set-up-to-fail-FINAL.pdf>.

[805] Проблемы, связанные с использованием полицейских данных, не являются уникальными для политики в области уголовного правосудия и обусловили необходимость ldемократической подотчетности в отношении управления данными и политики в Канаде. Контекст системной предвзятости и исторического угнетения в государственной практике сбора данных был признан, например, Инициативой по управлению данными коренных народов (BC FNDGI). БК ФНДГИ и ученые и защитники коренных народов призвали к суверенитету и участию коренных народов в отношении практики сбора данных. Уважение таких призывов имеет особое значение в свете того, как практика данных и обмена ими среди некоренного населения в Канаде "усилила системное угнетение, барьеры и неравные властные отношения»: Open North & British Columbia First Nations Data Governance Initiative, «Decolonizing Data: Indigenous Data Sovereignty Primer» (April 2017) at 3; Marcia Nickerson, «First Nations' Data Governance: Measuring the Nation-to-Nation Relationship» (May 2017). Both papers are available at <https://www.bcfndgi.com/>.

части 5 («Международные последствия алгоритмической полицейской деятельности в области прав человека и прав человека в соответствии с Хартией») настоящего доклада.

Таким образом, обсуждение социального и исторического контекста, только что представленное в этой части доклада – часть 2 («Социальный и исторический контекст»), – подчёркивает, что при рассмотрении вопроса о принятии новых методов полицейской деятельности, таких как алгоритмическая технология полицейской деятельности, крайне важно обеспечить, чтобы эти новые методы не усугубляли и не способствовали историческому ущербу, испытываемому общинами, подвергшимися системным предубеждениям.

Предотвращение увековечения системных предубеждений и дискриминации включает в себя постановку таких вопросов, как чья личная информация собирается или используется этой технологией, и какие люди или сообщества будут наиболее затронуты и почему? Использование сгенерированных полицией наборов данных,, которые подверженны влиянию предвзятости, может создавать отрицательные петли обратной связи, где лица из исторически неблагополучных общин помечаются алгоритмом как повышенный риск из-за исторической предвзятости по отношению к этим общинам.[806]

Если правоохранительные органы стремятся оправдать усиленную слежку или вмешательство в свободу и частную жизньна основе алгоритмических прогнозов, полученных из неявно предвзятых данных, это ставит исторически исторически находящихся в неблагоприятном положении под угрозу постоянной дискриминации. [807]

«Математика-стирка описывает как завышенное или ложное доверие к нейтральным математическим процессам, лежащим в основе процесса или метода принятия решений, как правило, чтобы скрыть скрыть погрешности в

---

[806] Например, в целом преступность чаще выявляется в общинах, которые находятся в центре внимания полиции. Кроме того, криминалисты привлекли внимание к проблемным последствиям несоразмерного внимания со стороны полиции и системы уголовного правосудия, которые сами по себе могут порождать экологические факторы, приводящие к дальнейшей целенаправленности действий полиции и криминализации. Наконец, социально-экономические различия и циклы нищеты делают людей уязвимыми для повышенного контроля и чрезмерной полицейской деятельности, в то время как они в меньшей степени способны получить доступ к результатам в уголовных судах, в которых основное внимание уделяется реабилитации, а не наказанию из-за нехватки финансирования юридической помощи.

[807] See, e.g., Elizabeth E Joh, «Feeding the Machine: Policing, Crime Data, & Algorithms» (2017) 26:2 William & Mary Bill of Rights Journal 287 at 292 <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1835&context=wmborj> and Chelsea Barabas (26 February 2019), Beyond Accuracy and Bias: The Pursuit of «Ethical AI» in Criminal Law, lecture presented at the University of Toronto Centre for Ethics, <https://c4ejournal. net/2019/03/01/chelsea-barabas-beyond-accuracy-and-bias-the-pursuit-of-ethical-ai-in-criminal-law-2019-c4ej-9/>. Влияние алгоритмической работы полиции на право на равенство и право на свободу от дискриминации исторически угнетенных общин дополнительно рассматривается ниже в разделе 5.4 ("Право на равенство и свободу от дискриминации").

принятии йрешений. Последствия этих рисков для прав человека и Устава ООН обсуждается в части 5 («Международные права человека и последствия хартии прав человека Алгоритмическая Полиция»).

Прежде чем перейти к более подробному объяснению того, что такое алгоритмические полицейские технологии и как они работают, приведём следующее яркое обсуждение в фокусе № 1: Перспективы сообщества в отношении алгоритмической полиции приводится краткое изложение выводов авторов в отношении мнений сообществ, которые, вероятно, будут наиболее затронуты принятием таких технологий.

В фокусе внимания № 1

Перспективы сообщества в области алгоритмической полиции

Для подготовки настоящего доклада были опрошены представители общин из групп, непропорционально пострадавших от чрезмерной криминализации, таких как чернокожие и коренные общины.[808] Среди этих представителей были: Джонатан Рудин, программный директор Юридической Службы аборигенов, автор книги «Коренные народы и система уголовного правосудия: справочник практикующего врача» и юрист, выступающий от своего имени в личном качестве; Десмонд Коул, канадский журналист, активист расовой справедливости и автор книги «Кожа, в которой мы находимся: год Черного сопротивления и власти»;

Центр правовых действий чернокожего населения (BLAC); и исследователь в Торонтском общественном сервис-провайде занимающемся вопросами уголовного правосудия.

Исследовательские интервью охватывали широкий круг точек зрения сообщества на алгоритмическую полицию и то, как такие технологии могут повлиять на соответствующие сообщества опрошенных. Эти лица подняли ряд проблем, которые тесно пересекаются с вопросами прав человека, связанными с алгоритмической полицией, рассмотренными в настоящем докладе, включая алгоритмическую предвзятость, проблемы с полицейскими данными, циклы обратной связи, закрепляющие системную дискриминацию, конфиденциальность данных, охлаждающее воздействие на расовую справедливость и активность в области прав коренных народов, обострение

[808] См. раздел 1.2 ("Методология") для получения подробной информации о протоколе исследования, использованном для этих интервью.

недоверия общин к правоохранительным органам. Их комментарии по этим вопросам включены в Часть 5 («Международные последствия алгоритмической полицейской деятельности в области прав человек и Хартии прав человека») настоящего доклада.

Прежде всего, представители сообщества выразили первостепенную озабоченность тем, что инструменты алгоритмической полиции будут увековечивать системную дискриминацию в отношении маргинализированых общин одновременно маскировка глубинных системных проблем и коренных проблем в системе уголовного правосудия, которые не могут быть решены с помощью технологии. По словам Десмонда Коула «предлагая более фантастический метод работы полиции профилирование – это не решение; на самом деле это стратегия продолжения профилирования чернокожих, коренных народов, и другие расовые группы. Я бы включил в это историческое нацеливание на странных и трансгендерных людей, люди, живущие с проблемами психического здоровья и люди, живущие с ограниченными возможностями»[809]. Реагируя на это понятие что алгоритмы могут уменьшить предвзятость, Черный Юридический Центр действий (BLAC) заявил: «Решение не в том, чтобы идти для алгоритма: «решение состоит в том, чтобы ваши офицеры и ваши сотрудники не были расистами. Прежде чем мы идите по этому пути, часть этих денег или все они могут быть вложены в то, что сообщает и изучает сказали, что навсегда важны-социальные детерминанты здоровья-правильно финансируемое образование система, общественное здравоохранение и тому подобное. Доступное жилье. Общественные центры, продуктовые магазины. Вовлечение сообщества в здравом смысле, а не идти к компьютеру, чтобы сказать вам, что есть проблема, и пусть частная компания извлекает из этого выгоду».[810]

Представители общин также рассматривали использование алгоритмических полицейских инструментов как неотделимое от канадской истории колониализма и системной дискриминации в отношении коренных, расовых и других маргинализированных групп населения. Ответы на интервью часто обращались к роли этой истории и её продолжающимся последствиям сегодня, включая историческую функцию правоохранительных органов и связанные с ней последствия для алгоритмической полиции. Например, Рудин поделился следующим личным мнением, выступая только от своего имени: «исторически сложилось так, что, когда коренные народы отстаивают свои права, они нарушают закон. Полиция используется историскии исторически я возвращаюсь к восстанию Риэля, но также Ока и Сожженная Церковь и Ипперваш и то, что происходит сейчас в Британской Колумбии – когда

[809] Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).
[810] Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

коренные народы отстаивают свои права, это не юридический вопрос для судов. Это вопрос полиции и полиция работает исходя из предположения, что коренные жители не имеют никаких прав и арестовываются по различным обвинениям. Коренные народы являются уязвимыми к этой слежке и сбору данных, когда, по сути, они занимаются законной деятельностью.[811] В своём интервью Коул заявил: «наследие нашего происхождения на этой территории, для меня, означает, что мы понимаем быть чёрным в Канаде через непрерывную историю которая насчитывает четыре столетия, будучи расовым, будучи другие, рассматриваемые как товар все, что вытекает из этого, каждый алгоритм, каждый технология распознавания образов просто вытекает из идеи о том, что существуют пределы нашим свободам как чёрные, так и коренные и другие расовые народы, и эти алгоритмы действительно помогают обеспечьте соблюдение ограничений».[812]

Представители общин, участвующие в пропаганде расовой справедливости, также разделяли мнение о том, что алгоритмические полицейские инструменты – это просто продолжение ранее существовавших полицейских инструментов, которые использовались для оправдания государственного насилия. Новые полицейские технологии рассматриваются, по словам Блэка, как позволяющие для научного способ оправдать то, что уже происходит [...] полиция находится в школах, или полиция находится на этом углу. Данные, оправдывающие большее исключение, большее наблюдение, большее взаимодействие с полицией. И мы точно знаем, что чёрные люди, чем больше они взаимодействуют с полицией, тем больше вероятность, что они умрут. [813] По словам Коула: «Возможность создать социальную сеть, которая говорит вам, что 13-летний подросток является частью банды, оправдает, когда ты подкатываешь к нему и выбиваешь из него все дерьмо. Я рисую прямую линию, потому что она проходит только через технологию, которую полиция пытается оправдать насилием, которое они совершают. Тридцать лет назад, когда у вас были только бумажные заметки, ваши бумажные заметки сказали бы вам, чтобы вы пошли за молодым человеком во всяком случае. Я на самом деле не отделяю эти технологии от полиции, участвующей в прямых формах насилия в отношении чернокожих общин». [814]

Опрошенные выразили сомнение в том, что алгоритмическая полиция может принести пользу маргинализированным общинам, и Рудин привел в

---

[811] Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019). Rudin also noted, with respect to police discretion: «In Toronto, Indigenous protest is generally well-tolerated. You let the police know in advance, we're going to shut down an intersection, and people don't react immediately by arrest, generally. But they could. You could see it as legitimate protest or as breaking the law. And the determination of that is not an analytic discussion; it's a policing perspective discussion».

[812] Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

[813] Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

[814] Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

качестве примера пропавших и убитых женщин и девочек из числа коренных народов «если я думаю о пропавших и убитых женщинах из числа коренных народов, я не знаю, что делает прогнозирование полиции. Их считают либо недостойными внимания, либо просто недостающими – так что же будет делать технология?»[815] Аналогично, исследователь из Торонто, занимающийся вопросами уголовного правосудия, заявил: «Я никогда в жизни не видел точечной карты насилия со стороны интимного партнёра. Существует ли точечная карта пропавших женщин из числа коренных народов?»[816]

Наконец, представители общин выразили озабоченность по поводу их недостаточного знакомства с новыми алгоритмическими методами полицейской деятельности и при этом подняли вопросы информационной асимметрии между полицейскими общинами, с одной стороны, и поставщиками правоохранительных органов и полицейских технологий – с другой.[817] В целом исследовательские интервью продемонстрировали значительный информационный и перспективный разрыв между представителями сообщества и представителями правоохранительных органов в отношении алгоритмических полицейских технологий.

Что такое алгоритмическая политика

Технология алгоритмической политики относится к разнообразным технологиям, управляемым алгоритмами, которые якобы позволяют правоохранительным органам делать выводы из массовой обработки данных с целью прогнозирования потенциальной незаконной деятельности (технологии «прогностической полиции») или, альтернативно, собирать и анализировать данные с помощью автоматизированного наблюдения и алгоритмического анализа («технология алгоритмического наблюдения»). В разделе 3.1 представлены технологические концепции, связанные с алгоритмической охраной порядка и затрагиваемые в настоящем докладе. В разделе 3.2 объясняется, чем алгоритмическая политика, как она определена в настоящем докладе, отличается как от обычных методов, так и от методов контроля и наблюдения за большими данными.

---

[815] Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019).

[816] Интервью исследователя из Торонто, поставщика общественных услуг, занимающегося вопросами уголовного правосудия, Иоланда Сон и Синтия Кхоо (8 May 2019).

[817] Исследователь из базирующегося в Торонто поставщика общественных услуг, занимающегося вопросами уголовного правосудия, поделился: "Было бы очень мало поставщиков общественных услуг (CSP), которые знакомы с такими вещами, как" горячая точка "полиции или автоматические инструменты принятия решений в целом". Исследователь выразил особую обеспокоенность по поводу того, "насколько неподготовленными и неинформированными являются большинство людей, таких как я и другие CSP. Мы просто не готовы. Интервью исследователя из Торонто, поставщика общественных услуг, занимающегося вопросами уголовного правосудия, Иоланда Сон и Синтия Кхоо (8 May 2019).

Технический праймер

В этом разделе дается основное объяснение технологическим концепциям, которые являются ключевыми для алгоритмической политики и обсуждаются на протяжении всего доклада.

Алгоритмическая полиция описывает использование алгоритмов полицейскими службами для упреждающего мониторинга и прогнозирования потенциальной преступности до того, как произошло какое-либо преступление. Этот термин охватывает средства наблюдения, такие как распознавание лиц и автоматические считыватели номерных знаков, которые полагаются на алгоритмические технологии. Она также включает в себя алгоритмические технологии, которые делают выводы с помощью массовой обработки данных в надежде предсказать потенциальную преступную деятельность. Последний тип технологии часто называют технологией предсказательной полиции. [818] Тем не менее, этот отчёт в основном использует термин «алгоритмическая полицейская технология», поскольку «прогностическая полицейская технология» является несколько неправильным термином: использование алгоритмов для получения выводов о потенциальной преступной деятельности приводит к обобщённым статистическим предположениям, а не конкретным прогнозам. Таким образом, авторы используют термин «алгоритмическая полиция», чтобы охватить как инструменты алгоритмического наблюдения, так и то, что в народе известно как «прогностическая полиция». [819] Последний термин будет использоваться позже в настоящем докладе, когда речь пойдёт конкретно о технологиях «прогностической полиции». Это использование признаёт, что для общественности прогнозирующая полицейская деятельность остаётся более популярным и привычным термином для описания типов рассматриваемых технологий. Это использование также отличает технологии алгоритмической полиции с предполагаемыми прогностическими

---

[818] В настоящем докладе используется термин "прогнозирование политики", где это уместно, для обозначения тех технологий, которые пытаются генерировать статистические догадки посредством массовой обработки данных.

[819] «Прогнозирующая полиция - это маркетинговый термин, популяризированный поставщиками в отрасли общественной безопасности, для компьютерных систем, которые используют данные для автоматического прогнозирования того, где произойдет преступление или кто будет участвовать". Подъем, застрявший в образце: ранние доказательства "прогнозирующей полиции" и гражданских прав.» Upturn, Stuck in a Pattern: Early evidence on «predictive policing» and civil rights (August 2016), at 2 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_StuckJn_a_Pattern_v.1.01.pdf>. S/ Констебль Райан Прокс (Ryan Prox) из Департамента полиции Ванкувера, в своем исследовательском интервью, также критически отозвался о термине "прогнозирующая полиция": "Я думаю, что это маркетинговая уловка многих поставщиков, которые говорят, что они могут делать все эти другие вещи. Но многое из этого - черные ящики, где нет истинной оценочной метрики о том, обеспечивают ли они какие-либо результаты по предупреждению преступности. Я не верю, что они ". Интервью Райана Прокса Синтии Хоо и Йоланды Сонг (7 May 2019).

возможностями от алгоритмических полицейских технологий, которые используются для общего наблюдения.

Алгоритм – это «технологически автоматизированная математическая формула»,[820] которая предписывает компьютеру обрабатывать заданные входные данные определенным образом, чтобы получить определённые выходные данные. Там, где алгоритм полагается на помощь или замену человеческого принятия решений, это приложение известно, как алгоритмическое принятие решений, или иногда автоматизированное принятие решений. Алгоритмы занимают центральное место в ИИ, который относится к способности компьютера выполнять задачи, которые обычно считаются требующими человеческого интеллекта.[821]

Некоторые алгоритмы, такие как алгоритмы машинного обучения, автономно «учатся»[822] выполнять задачи. Алгоритмы генерируют набор правил, основанных на больших наборах, обучающих данных, и алгоритм автономно обновляет эти правила по мере поступления большего количества данных для оптимизации алгоритмических выходов в направлении конкретной цели. [823] Машинное обучение частично опирается на интеллектуальный анализ данных, который представляет собой «практику поиска больших объёмов компьютеризированных данных для поиска полезных моделей и тенденций.»[824] Алгоритмы экстраполируют паттерны из примеров обучающего набора для получения выходных данных (выходов) из новых входных данных (входов). По мере поступления новых данных алгоритмы могут изменяться в соответствии с новыми данными.[825] Компьютерное зрение (распознавание визуальных

---

[820] Королевский институт объединенных служб, алгоритмы машинного обучения и принятие решений полицией: правовые, этические и нормативные проблемы (September 2018) at 2. <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

[821] Компьютеры, которые выполняют определенные дискретные задачи, такие как игра в шахматы, разблокировка дверей автомобиля или автозаполнение поисковых терминов, демонстрируют искусственный узкий интеллект. С другой стороны, искусственный общий интеллект относится к "системе, которая отображает интеллект во многих областях, с возможностью обучения новым навыкам, и которая имитирует или даже превосходит человеческий интеллект»: Privacy International, «Privacy and Freedom of Expression In the Age of Artificial Intelligence» (April 2018), at 6 <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf>.Рассматриваемые в настоящем докладе технологии полицейской деятельности и уголовного правосудия представляют собой искусственные узкие системы разведки.

[822] Ясно, что "идея о том, что компьютеры "учатся", в значительной степени является метафорой и не подразумевает, что компьютерные системы искусственно воспроизводят передовые когнитивные системы, которые, как считается, участвуют в обучении человека.» Harry Surden, «Machine Learning and Law» (2014) 89: 1 Washington Law Review 87 at 89.

[823] Королевское общество, машинное обучение: сила и обещание компьютеров, которые учатся на примере (April 2017) at 19 <https://royalsociety. org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf>. «Learning» is used metaphorically to represent the process of the computer adjusting its algorithm as more data is provided.

[824] Walter L Perry et al, «Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations» (2013) at 34 <https://www.rand. org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf>, citing the Merriam-Webster online dictionary. Note that while machine learning involves data mining, it is possible to engage in data mining without the use of machine learning.

[825] Алгоритмы машинного обучения могут быть объединены и интегрированы друг с другом в сотни уровней

образов), обработка естественного языка (интерпретация и моделирование человеческого языка) и распознавание речи (преобразование произносимых слов в текст) являются общими примерами технологии машинного обучения. [826]

Существует два вида машинного обучения: контролируемое и неконтролируемое. При контролируемом машинном обучении набор обучающих данных маркируется.[827] Например, алгоритм может быть проинструктирован анализировать тысячи фотографий животных, уже помеченных как «собака» или «кошка», чтобы обучить его различать их. Алгоритм определяет, какие факторы отличают фотографии собак от фотографий кошек, и применяет эти правила к новым, немаркированным фотографиям (входы), чтобы классифицировать их (выходы). При неконтролируемом машинном обучении система ищет закономерности в немаркированных обучающих данных (например, немаркированных фотографиях) на основе переменных, которые она определяет как наиболее релевантные, и впоследствии генерирует правила на основе этих закономерностей. [828]

Внутренняя работа алгоритмов машинного обучения не всегда понятна человеческому пониманию, или их исходный код может быть скрыт от общественности по причинам коммерческой тайны в интеллектуальной собственности или из-за соглашений о свободной торговле. Эта непрозрачность приводит к тому, что обычно называют проблемой чёрного ящика[829]: можно видеть входные и выходные данные, но практически нет информации о том, как или почему данный вход приводит к определённом выходу. Это отсутствие объяснимости может быть проблематичным, когда оно ухудшает способность оценивать надёжность данного алгоритма, включая обнаружение того, работает ли алгоритм ошибочным или непреднамеренным образом. Например, в одном

алгоритмической обработки данных, формируя нейронные сети. Нейронная сеть - форма архитектуры машинного обучения, которая состоит из многочисленных уровней взаимосвязанных вычислительных блоков обработки. Каждый уровень обрабатывает входные данные, которые он получает, и выходные данные, которые этот уровень предоставляет, становятся входными данными для следующего уровня блоков обработки. Таким образом, каждый начальный вход в нейронной сети проходит через десятки-сотни уровней алгоритмической обработки до появления конечного выхода. Этот процесс известен как глубокое обучение. "Доступ сейчас", "Права человека в эпоху искусственного интеллекта", 9 лет; "Что такое нейронная сеть и чем ее работа отличается от работы цифрового компьютера? (Другими словами, мозг как компьютер?)", Scientific American (14 May 2007) <https://www.scientificamerican.com/article/experts-neural-networks-like-brain/>; and Hannah Couchman, «Policing by Machine: Predictive policing and the threat to our rights,» (January 2019) Liberty, at 11 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.

[826] Access Now, Human Rights in the Age of Artificial Intelligence (November 2018) at 10 <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

[827] Royal United Services Institute, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges (September 2018) at 18<https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

[828] Ibid, at 18-19.

[829]Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Cambridge, Massachusetts: Harvard University Press, 2015) at 3.

исследовании нейронная сеть, которая якобы научилась различать собак и волков, точно классифицировала фотографии, но на основе того, был ли снег на заднем плане, а не на основе особенностей животных.[830]

Чтобы быть эффективными, алгоритмы должны быть обучены на данных, которые являются точными и репрезентативными для изучаемого предмета. Когда набор обучающих данных является неточным или предвзятым, эти недостатки отражаются на выходных данных алгоритма (даже если недостатки не очевидны при оценке выходных данных алгоритма). Этот принцип обычно называют «мусор на входе, мусор на выходе». Например, если обучающие фотографии кошек и собак помечены неправильно, алгоритм будет классифицировать входные фотографии менее точно. Кроме того, если алгоритм обучен на тысячах фотографий кошек и только на десяти фотографиях собак, он сможет классифицировать фотографии кошек более точно, чем фотографии собак. Это пример статистического искажения, которое относится к пробелам или другим проблемам в наборе данных, которые заставляют его быть нерепрезентативным к реальности. Статистическая предвзятость является основным источником беспокойства в реальных наборах учебных данных.[831] Яркий пример можно увидеть в алгоритмах распознавания лиц, которые обучаются на наборах данных, в которых определённые пол, возраст или расовые группы недостаточно представлены или отсутствуют. Такие модели будут делать больше ошибок в распознавании лица отдельных лиц из этих недопредставленных групп.[832]

Технологии алгоритмического контроля, в основе которых лежат алгоритмы, обученные на исторических данных, будут пытаться прогнозировать будущие результаты на основе этих данных, и, таким образом, они будут генерировать выводы, основанные на прошлых паттернах. Основное

---

[830] Marco Tulio Ribeiro, Sameer Singh & Garlos Guestrin, «'Why Should I Trust You?' Explaining the Predictions of Any Classifier» (Paper delivered at KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2016). For additional examples of artificial intelligence technically following developers' instructions but in ways that «subverted their expectations or intentions», see Joel Lehman, Jeff Clune & Dusan Misevic, «The Surprising Creativity of Digital Evolution: A Collection of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities» (2020) Artificial Life 1.

[831] Upturn, Stuck in a Pattern: Early evidence on «predictive policing» and civil rights (August 2016) at 6 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf>.

[832] Joy Buolamwini & Timnit Gebru, «Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification», (2018) 81 Proceedings of Machine Learning Research 1, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Brendan Klare, Mark Burge, Joshua Klontz, et al, «Face Recognition Performance: Role of Demographic Information», (2012) 7(6) IEEE Transactions in Info Forensics & Security 1789, <https://ieeexplore.ieee.org/document/6327355>. Аналогичным образом, в программах алгоритмического контроля существующие данные о деятельности полиции могут использоваться при обработке данных для получения выводов относительно риска, так что данные о деятельности полиции становятся прокси для данных о прошлой преступной деятельности, даже если они являются двумя очень разными метриками. Другими словами, данные полиции, как правило, отражают поведение правоохранительных органов, а не отражают истинное положение дел с преступной деятельностью и то, кто именно. Более подробную информацию о том, как данные полиции неточно или точно отражают преступную деятельность, см. в разделе 2.2. («Bias and Inaccuracies in Police Data»).

предположение состоит в том, что модели, найденные в прошлых данных, будут по-прежнему применимы в будущем. Однако там, где исторические данные искажаются неправомерным чрезмерным представлением и системной дискриминацией, результирующие модели будут воспроизводить эти искажения. Это особенно важно, потому что алгоритмы способны обнаруживать только корреляцию, а не причинно-следственную связь. Если алгоритм контроля был загрязнён повреждёнными, искажёнными, неполными или предвзятыми данными (непреднамеренно или намеренно), он был обучен на грязных данных.[833]

При разработке и применении алгоритмов машинного обучения обеспечение точности и непредвзятости обучающих данных является лишь одним из компонентов непрерывного процесса, который должен осуществляться для правильной оценки точности и надёжности алгоритма и обеспечения того, чтобы он применялся таким образом, чтобы не приводить к неблагоприятным результатам или предвзятости в отношении лиц, подвергнутых воздействию алгоритма.

Оценка и функционирование механизма машинного обучения может быть столь же чревато, как и процесс обучения. Тестирование и оценка должны проводиться на основе входных данных, которые будут использоваться в оперативных ситуациях реального времени. Алгоритм, который может показаться точным и непредвзятым, все ещё может давать неблагоприятные результаты, если в процессе работы вводятся новые и непроверенные типы данных. Оперативные входные данные также должны быть точными; в противном случае могут возникнуть неблагоприятные результаты, даже если сам алгоритм кажется в целом надёжным. По этой причине тестирование и оценка также должны продолжаться после этапа внедрения.

В разделе 3.1 представлены основные понятия, которые используются в последующих частях настоящего доклада. Эти объяснения помогают облегчить понимание результатов исследований и правового анализа, касающихся технологии алгоритмической полиции, изложенных в части 4 («Алгоритмическая полиция в Канаде: современный ландшафт») и части 5 («Международные последствия алгоритмической полиции в области прав человека и прав человека в соответствии с Хартией»).

---

[833] Ричардсон, Шульц и Кроуфорд переняли термин "грязные данные" из области интеллектуального анализа данных, где термин означает отсутствующие, ошибочные или непоследовательно представленные данные: Rashida Richardson, Jason M Schultz & Kate Crawford, «Dirty Data, Bad Predictions: How civil rights violations impact police data, predictive policing systems, and justice» (May 2019) 94:192 New York University Law Review 193 at 195, <https://www. nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>.

Завершая часть 3, раздел 3.2 контекстуализирует алгоритмические полицейские технологии по отношению к традиционным полицейским методам.

Чем отличается алгоритмическая полиция?

Алгоритмическое управление связано с методами управления большими данными, которые используются наряду с традиционными методами управления, но отличаются от них. Инфраструктура государственного надзора и экосистема больших данных правоохранительных органов формируют фон и топливо для алгоритмических полицейских технологий.

Сегодня полицейские службы Канады имеют доступ к беспрецедентным и постоянно растущим объёмам данных. Полицейские службы используют различные взаимосвязанные системы для отслеживания преступной деятельности, структуры преступлений, подозреваемых и жертв и расследован.[834] Благодаря сбору и отслеживанию данных правоохранительными органами был создан ряд муниципальных, региональных, провинциальных и федеральных баз данных и систем внутреннего делопроизводства.[835]

С течением времени методы сбора и агрегирования данных эволюционировали с появлением новых технологий. Для примера, правоохранительные органы искали доступ к данным «умного города»,[836]

---

[834]Например, в Британской Колумбии все провинциальные и муниципальные органы полиции используют централизованную провинциальную систему ведения документации (CPK), известную как Полицейская система управления информацией (PRIME-BC). Кроме того, органы муниципальной полиции также имеют доступ к комплексной системе сбора и анализа данных, известной под названием "Сводные данные и разведывательная горнодобывающая среда" (CRIME), которая управляется и управляется Департаментом полиции Ванкувера. Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019); see also Jun Min Chang, «Vancouver C.R.I.M.E. System» (1 August 2013) Blue Line <https://www.blueline.ca/vancouver_c-r-i-m-e-_system-2784/>.

[835] К таким базам данных относятся, например, Канадский полицейский информационный центр (CPIC), Полицейский информационный кооператив Онтарио (OPTIC) или Ниш, Полицейский информационный портал (PIP) и Полицейская информационная система (PIRS), Канадские службы идентификации уголовных преступлений в реальном времени (CCRTIS): See Alison Brooks, «Law Enforcement Information Management Study» (October 2014) IDC at 12-22, <https://cacp.ca/index.html?asst_id=977>. В целом эти базы данных предназначены для хранения и обмена информацией о судимости, непогашенных обвинениях, ордерах, лицах, представляющих интерес, похищенном имуществе, личных флагах с целью предупреждения сотрудников полиции, которые могут взаимодействовать с ними, и другой интересующей информации.

[836] Например, электронные транзитные пропуска в нескольких канадских городах привели к тому, что их соответствующие транзитные агентства без ордера поделились с полицией частными данными о поездках пригородов: Ben Spurr, «Metrolinx has been quietly sharing Presto users' information with police» (3 June 2017) The Toronto Star <https://www.thestar.com/news/gta/2017/06/03/metrolinx-has-been-quietly-sharing-presto-information-with-police.html>; CBC News, «Police use of Compass Card data raises alarm for B.C. civil liberties advocate» (9 August 2017) <https://www.cbc.ca/news/canada/british- columbia/police-use-of-compass-card-data-raises-alarm-for-b-c-civil-liberties-advocate-1.4240452>; Jacques Marcoux, «Winnipeg Transit gave Peggo card travel history to police without warrants» (7 June 2017) CBC News <https://www.cbc.ca/news/canada/manitoba/winnipeg-transit- peggo-data-

данным социальных сетей,[837] информации о мобильных устройствах (включая местоположение), полученной удалённо, и потребительским данным частного сектора (таким как камеры наблюдения, встроенные в устройства «умного дома»).[838]

Методы управления большими данными характеризуются тремя центральными признаками, которые используются для того, чтобы отличить большие данные в целом от предшествующих методов обработки данных и, таким образом, отличить политику больших данных от обычных методов управления. [839]Эти функции известны как «три против», каждая из которых относится к беспрецедентному масштабу компонента: объем (огромные объёмы данных собираются и обрабатываются в правоохранительных целях, далеко за пределами того, что человек мог бы обрабатывать вручную или что может обрабатывать традиционное программное обеспечение, не связанное с ИИ); скорость (правоохранительные органы могут обрабатывать данные наблюдения и полиции с беспрецедентной скоростью, вплоть до реального времени); и разнообразие (множество различных типов наборов данных теперь доступны полиции для использования в мониторинге и расследованиях из различных источников, которые могут быть интегрированы друг с другом, объединены и перекрёстно связаны, чтобы привести к более глубоким, более детальным или более глубоким выводам и выводам).[840]

---

police-1.4148965>; see also Teresa Scassa, «As smart cities become our norm, we must be smart about a data strategy» (13 February 2019) Hill Times <https://www.hilltimes.com/2019/02/13/smart-cities-become-norm-must-smart-data-strategy/188280>.

[837] Эта возможность обеспечивается с помощью устройств отслеживания международной идентификации мобильного абонента (IMSI), также известных как имитаторы сотовых станций, которые представляют собой «устройства, олицетворяющие вышки сотовых телефонов, убеждающие мобильные устройства взаимодействовать с ними, поскольку они обычно взаимодействуют только с башней поставщика услуг»: Tamir Israel & Christopher Parsons, Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada (August 2016) at 2, <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>. Police services in Calgary, Winnipeg, and Toronto, as well as the Ontario Provincial Police and RCMP have all been confirmed to use or have used IMSI catchers, thus indiscriminately collecting data from all cellphones within range: Matthew Braga & Dave Seglins, «Cellphone surveillance technology being used by local police across Canada» (13 April 2017) CBC News <https://www.cbc.ca/news/technology/cellphone-surveillance-police-canada-imsi-catcher-privacy-1.4066527>; Kate Allen, Jayme Poisson & Wendy Gillis, «Two years after they said they didn't, Toronto police admit they use Stingray cellphone snooping device» (5 March 2018) The Toronto Star, <https://www.thestar.com/news/gta/2018/03/05/two-years-after-they-said-they-didnt-toronto-police-admit-they- use-stingray-cellphone-snooping-device.html>.

[838] See, e.g., Jennifer Valentino-DeVries, «Google's Sensorvault Is a Boon for Law Enforcement. This is How It Works» (13 April 2019) New York Times <https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html>; Sam Biddle, «Amazon's Home Surveillance Chief Declared War on 'Dirtbag Criminals' as Company Got Closer to Police» (14 February 2019) The Intercept <https://theintercept.com/2019/02/14/amazon-ring-police-surveillance/>.

[839] See e.g., Alison Brooks, «Law Enforcement Information Management Study», IDC (October 2014) <https://cacp.ca/index.html?asst_id=977>, at 6-7; Greg Ridgeway, «Policing in the Era of Big Data» (2018) 1 Annual Review of Criminology 401 at 402-03; and «3D Data Management: Controlling Data Volume, Velocity, and Variety», META Group (6 February 2001). <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D- Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.

[840] Следует отметить, что в докладе Управления Комиссара по информации Соединенного Королевства говорится: "Недавно некоторые предположили, что определение трех Vs устало из-за чрезмерного использования и что существуют многочисленные формы больших данных, которые не все имеют одинаковые

Технологии алгоритмического контроля отличаются как от традиционных, так и от методов контроля больших данных и требуют особого внимания и заботы.[841] Во-первых, такие технологии выводят методы управления большими данными на еще более высокий уровень масштабирования. Большие источники данных, с их огромным объёмом и диапазоном информации, поддерживают алгоритмические технологии, которые могут использовать власти. Как поделился в интервью представитель Лаборатории прогнозной аналитики полиции Саскачевана (SPPAL)», «в прошлом я не смог бы использовать [алгоритмическое моделирование], потому что у меня не было бы объёма данных или статистических возможностей».[842]Во-вторых, алгоритмические методы обеспечивают более широкий диапазон сбора, агрегирования и анализа данных, чем обычные методы или методы контроля больших данных. Например, методы наблюдения, которые алгоритмически автоматизированы для выполнения различных задач, связанных со сбором, агрегированием и анализом данных (таких как распознавание лиц, мониторинг социальных сетей и анализ социальных сетей), менее ограничены затратами и ресурсами по сравнению с традиционными методами. Институт ИИ теперь формулирует различие между алгоритмическим и традиционным наблюдением следующим образом:

ИИ повышает ставки в трёх областях: автоматизация, масштаб анализа и способность к прогнозированию. В частности, системы ИИ позволяют автоматизировать возможности наблюдения далеко за пределами человеческого обзора и ручной аналитики. Таким образом, они могут служить дальнейшей централизации этих возможностей в руках небольшого числа действующих лиц. Эти системы также экспоненциально масштабируют анализ и отслеживание больших объёмов данных, пытаясь установить связи и выводы, которые были бы трудными или невозможными до их внедрения. Наконец, они предоставляют новые прогностические возможности для определения индивидуальных особенностей и профилей риска, повышая возможность детального контроля численности населения.[843]

черты. Хотя нет однозначного определения больших данных, мы считаем полезным рассматривать их как данные, которые из-за нескольких различных характеристик трудно анализировать с использованием традиционных методов анализа данных». «Big data, artificial intelligence, machine learning and data protection» (4 September 2017) United Kingdom Information Commissioner's Office, at 6 (footnotes omitted) <https://ico.org.uk/media/for-organisations/documents/2013559/ big-data-ai-ml-and-data-protection.pdf>. Признавая это, характеристика "три Vs" остается полезной для целей настоящего доклада и различает, в частности, обычную политику, политику больших данных и алгоритмическую политику. See, e.g., Greg Ridgeway, «Policing in the Era of Big Data» (2018) 1 Annual Review of Criminology 401 at 402-03, describing the role of big data in policing based on these traits.

[841] Upturn, Stuck in a Pattern: Early evidence on «predictive policing» and civil rights (August 2016) at 1 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_I n_a_Pattern_v.1.01.pdf>.

[842] Интервью представителя Saskatchewan Police Predictive Analytics Lab Синтии Кхоо (23 July 2019).

[843] AI Now Institute, AI Now Report 2018 (December 2018) at 12 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

Прозрачность, окружающая алгоритмические технологии контроля, также отличается от традиционных методов контроля и больших данных. Инструменты, управляемые алгоритмами, часто являются чёрными ящиками, в отличие от обычных инструментов. Например, актуарные оценки рисков, разработанные и подтверждённые социологами, уже много лет используются в контексте исправительных учреждений и вынесения приговоров в Канаде,[844] а также в системах уголовного правосудия в других юрисдикциях,[845] хотя и не без критики и споров.[846] Эти оценки могут быть объяснены и оценены социологами, включая то, какие конкретные факторы были включены и какой вес был придан любому конкретному фактору. Алгоритмы машинного обучения, с другой стороны, могут генерировать и следовать правилам, которые не видны человеческим наблюдателям. В результате люди могут оказаться неспособными определить, какие факторы учитываются алгоритмом машинного обучения или как они взвешиваются.[847]

Даже эксперты могут быть не в состоянии проанализировать сотни или тысячи шагов в конкретном алгоритме или множество точек данных, которые алгоритм использует, чтобы прийти к определённому результату.[848]Результатом является то, что технологии алгоритмической полиции могут использовать математические системы для того, чтобы прийти к выводам, которые совершенно непрозрачны для разработчиков систем, тех, кому поручено использовать выходные данные в правоохранительных органах и уголовном правосудии, или тех, на кого влияют технологии алгоритмической полиции.

---

[844] See, e.g., Ewert v Canada, 2018 SCC 30 at para 11.

[845] Royal United Services Institute, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges (September 2018) at 6 <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

[846] See e.g., Ewert v Canada, 2018 SCC 30; Margaret Shaw & Kelly Hannah-Moffat, «Gender, Diversity And Risk Assessment In Canadian Corrections» (September 2000) 47:3 Probation Journal 163.

[847] «Более продвинутые алгоритмические системы, которые включают в себя подходы к машинному обучению, используются с проблемами, когда ранее существовавшие правила или теории плохо улавливают желаемые отношения» вход-выход ". В результате машины создают взаимосвязь между входами и выходами в обратном направлении от данных, обычно без учета интерпретируемости человеком. В некоторых случаях это может позволить машинам создавать гораздо более эффективные соединения "вход-выход" - какие предсказания компьютерного учёного - чем могли бы создавать ручные системы на основе правил». Michael Veale, «Algorithms in the Criminal Justice System» (June 2019), Law Society of England and Wales at 10 <https://www.lawsociety.org.uk/support-services/research- trends/algorithm-use-in-the-criminal-justice-system-report/>.

[848]«Эти новые системы выходят за рамки простого оказания помощи аналитикам по человеческим преступлениям в обобщении данных. Они направлены на автоматическое прогнозирование будущих преступлений в целях принятия решений полицией. Для этого эти системы выносят суждения о том, что означают эти данные - например, указывая на то, что люди, скорее всего, будут причастны к насильственным преступлениям в будущем, или взвешивая сотни или тысячи факторов таким образом, что ни один человеческий аналитик не может в полной мере понять ". Upturn, Stuck in a Pattern: Early evidence on «predictive policing» and civil rights (August 2016) at 2 <https://www.upturn.org/static/reports/2016/stuck- in-a-pattern/files/Upturn_-_Stuck_I n_a_Pattern_v.1.01.pdf>.

Алгоритмическая полиция в Канаде: современный ландшафт

Технологии алгоритмической полицейской деятельности присутствуют или рассматриваются на всей территории Канады в форме как прогностической полицейской деятельности, так и алгоритмических средств наблюдения. В течение последнего десятилетия стратегические планы полицейских служб, бюджетные документы и ежегодные отчёты отражали планы внедрения алгоритмических методов полицейской деятельности под такими терминами, как «прогнозная», «управляемая данными» или «управляемая разведкой» полицейская деятельность, подкреплённая большим акцентом на аналитику данных.[849] Некоторые полицейские службы приступили к экспериментальному внедрению и внедрению алгоритмических полицейских систем[850] или выразили заинтересованность в ходе исследовательских интервью, проведённых для настоящего доклада, что усиливает растущий интерес среди правоохранительных органов в целом.[851]

Технологии алгоритмической полицейской деятельности присутствуют или рассматриваются на всей территории Канады в форме как прогностической полицейской деятельности, так и алгоритмических средств наблюдения. В течение последнего десятилетия стратегические планы полицейских служб, бюджетные документы и ежегодные отчёты отражали планы внедрения алгоритмических методов полицейской деятельности под такими терминами, как «прогнозная», «управляемая данными» или «управляемая разведкой» полицейская деятельность, подкреплённая большим акцентом на аналитику данных. Некоторые полицейские службы приступили к экспериментальному внедрению и внедрению алгоритмических полицейских систем или выразили заинтересованность в ходе исследовательских интервью, проведённых для настоящего доклада, что усиливает растущий интерес среди правоохранительных органов в целом.

---

[849] See, e.g., Winnipeg Police Service 2011 Annual Report at page 9; London Police Service 2013 Annual Report at page 17, https://www. londonpolice.ca/en/About/resources/Documents/2013-Annual-Report.pdf; Peel Regional Police 2017 Budget Document at pages 4 and 11, https:// www.peelpoliceboard.ca/en/board-meetings/resources/2017-Peel-Regional-Police-Budget.pdf; Ottawa Police Service June 2018 Modernization Roadmap Report at page 10, http://app05.ottawa.ca/sirepub/agdocs.aspx?doctype=agenda&itemid=375842; Edmonton Police Service 2018 Annual Policing Plan at pages 5 and 6, https://edmontonpolicecommission.com/wp-content/uploads/2019/03/2018-Annual-Policing-Plan.pdf

[850] Matt Meuse, «Vancouver police now using machine learning to prevent property crime» (22 July 2017) CBC News <https://www.cbc.ca/news/ canada/british-columbia/vancouver-predictive-policing-1.4217111>; Meaghan Craig, «Saskatoon police lead the country with Predictive Analytics Lab» (15 January 2016) Global News <https://globalnews.ca/news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/>.

[851] See e.g., Peter Sloly, «Emerging tech that can make smart cities safer», Blue Line (8 October 2018) <https://www.blueline.ca/emerging-tech- that-can-make-smart-cities-safer-5710/>; Cory Schactel, «More Data, More Problems», Avenue Magazine Edmonton (5 June 2019) <https://www. avenueedmonton.com/innovation/more-data-more-problems/>; and Richard Boire, «Data-Driven Decisions for Law Enforcement in Toronto», Machine Learning Times (17 August 2018) <https://www.predictiveanalyticsworld.com/machinelearningtimes/data-driven-decisions-for-law- enforcement-in-toronto/9640/>.

В каждом из следующих разделов рассматриваются инициативы и практика алгоритмической полицейской деятельности, осуществляемые полицейскими службами Канады: ориентированные на местоположение алгоритмические полицейские технологии (раздел 4.1), ориентированные на человека алгоритмические полицейские технологии (раздел 4.2) и алгоритмические полицейские методы наблюдения (раздел 4.3). В разделе 4.4 обсуждаются ограничения результатов исследований, а в разделе 4.5 приводится резюме и анализ результатов исследований, касающихся современного ландшафта алгоритмической полиции в Канаде. В этой части доклада (часть 4) основное внимание уделяется изложению фактического ландшафта как такового в той мере, в какой его могли бы определить авторы; анализ и критические последствия этих технологий представлены далее в части 5 («Международные последствия алгоритмической полицейской деятельности в области прав человека и прав человека в соответствии с Хартией»).

В некоторых случаях данная технология может использоваться для других возможностей, помимо алгоритмических предсказаний, таких как организация и связывание данных, без составления алгоритмических предсказаний на основе этих данных. Однако нынешнее обладание этим потенциалом канадскими правоохранительными органами также считается актуальным и входит в сферу охвата настоящего доклада. В каждом разделе даётся ссылка на параллельные примеры в коллегиальных юрисдикциях, чтобы дополнительно проиллюстрировать потенциальное использование и риски каждой рассматриваемой технологии.

Чтобы завершить это введение в Часть, в следующем выделенном блоке № 2: «Обзор канадской системы уголовного правосудия» содержится информация о структуре и процессе работы правоохранительных органов и системы уголовного правосудия в Канаде. Этот контекст помогает продемонстрировать, как алгоритмические полицейские технологии вписываются в канадскую правоохранительную систему и систему уголовного правосудия.

В фокусе внимания № 2

Обзор канадской системы уголовного права

В канадской федеральной системе управления каждый уровень управления – федеральный, провинциальный территориальный и муниципальный – играет определённую роль в системе уголовного правосудия.

Федеральное правительство несёт ответственность за разработку и реформирование уголовно-правовых норм, предусмотренных Уголовным кодексом и другими федеральными законами, такими как закон о контролируемых наркотиках и в провинции имеют полномочия создавать полицейские силы, органы прокуратуры, службы условно-досрочного освобождения и другие соответствующие учреждения, такие как программы компенсации жертвам.

С согласия провинций и территорий полицейские службы были созданы на основе делегированных полномочий во многих муниципалитетах Канады (таких, как Ванкувер, Калгари и Торонто) и в общинах коренных народов. В провинции Онтарио и Квебек действуют полицейские службы (провинциальная Полиция Онтарио и Квебекская полиция). Королевская канадская конная полиция (КККП) – это национальная полицейская служба, которая обслуживает оставшиеся районы, которые ещё не охраняются полицейскими службами коренных народов, провинций или муниципалитетов. Там, где действует КККП, она делает это в силу делегированных полномочий провинциалы или территориального правительства в этой области.

Некоторые особенности уголовных расследований и уголовного судопроизводства, как правило, схожи в Канаде. Это сходство отчасти объясняется тем, что в Канаде действует единый свод уголовных законов по всей стране и что все правоохранительные органы и королевские прокуроры должны действовать в конституционных рамках канадской Хартии прав и свобод.[852] Однако, несмотря на то, что большая часть системы уголовного правосудия в Канаде одинакова, выбор местной или региональной политики и ограниченность ресурсов означают, что некоторые виды полицейской практики или качество доступа к правосудию могут отличаться в разных странах Канады.

Основные этапы уголовного расследования и судопроизводства в Канаде заключаются в следующем:

1. Полицейские службы проводят расследования в отношении людей, собирая информацию и доказательства.

2. Сотрудники полиции обладают ограниченными полномочиями по ограничению свободы подозреваемых в ходе уголовного расследования (т.е. следственными полномочиями по задержанию и аресту). Незаконное осуществление этих полномочий, таким образом, нарушает права Хартии.

3. После сбора имеющихся доказательств полиция может предъявить обвиняемому уголовное обвинение (или обвинения), если у следователя

---

[852] Канадская хартия прав и свобод, статья 7, часть I Закона о Конституции 1982 года, включенная в приложение B к Закону о Канаде 1982 (UK), 1982, c 11.

имеются разумные и вероятные основания полагать, что данное лицо совершило преступление.

4. Если предъявлено уголовное обвинение, то должно быть определено, будет ли обвиняемый освобождён или будет содержаться под стражей до суда, пока уголовные обвинения будут проходить через систему уголовного судопроизводства (залог).

В зависимости от обстоятельств (например, характера преступления или предшествующей судимости обвиняемого) обвиняемый либо освобождается на месте ареста арестовывающим должностным лицом (например, на обочине дороги), либо освобождается из полицейского участка (например, после рассмотрения дела), либо освобождается из уголовного суда под залог мировым судьёй.

5. После предъявления обвинения уголовное производство начинается в суде. Прокуроры берут дело под свой контроль и получают доказательства от следственной полицейской службы.

6. Все лица, находящиеся в суде, считаются невиновными. Уголовное судопроизводство завершается следующими способами:

а) снятием или приостановлением обвинений короной;

б) участием подсудимого в диверсионной программе до снятия или приостановления обвинения (приостановленные или снятые обвинения означают, что лицо невиновно в предъявленных обвинениях);

в) признанием подсудимым своей вины и соответствующим отказом от права на судебное разбирательство по существу;

г) уголовным разбирательством, в котором обвиняемый считается невиновным и должен быть оправдан, если обвинение не докажет вину (предъявленных обвинений) вне разумных сомнений перед судьёй или присяжными.

7. Уголовное наказание назначается в том случае, если лицо признается виновным в совершении преступления либо в результате признания своей вины, либо в результате признания его виновным в уголовном процессе.

8. Может иметь место целый ряд процессов, связанных с любым вынесенным уголовным приговором, включая условно-досрочное освобождение, тюремное заключение и условно-досрочное освобождение.

9. После установления вины и вынесения приговора подсудимый имеет право обжаловать вынесенный приговор.

10. После отбытия уголовного наказания канадский Совет по условно-досрочному освобождению управляет канадской системой определения того, существует ли какое-либо приостановление судимости (ранее называвшееся помилованием).[853]

Правоохранительные органы расследуют и собирают доказательства с помощью широкого спектра методов и процессов. Некоторые полицейские расследования носят оперативны характер (например, реагирование на звонок 911), в то время как другие носят упреждающий характер и пытаются обнаружить преступление без явной просьбы о помощи со стороны сообщества. Чтобы построить уголовное дело, правоохранительные органы могут полагаться на множество различных источников информации, таких как показания свидетелей, записанные разговоры (например, копии текстовых сообщений или электронных писем или перехваченная запись телефонного звонка), видеозаписи камер видеонаблюдения, деловые записи или наблюдения.

Все методы должны осуществляться в рамках Конституции, хотя на практике многие расследования в конечном счёте оказываются неконституционными в том или ином отношении. Устав предусматривает право добиваться исключения неконституционно полученных доказательств. [854] Однако полученные данные и методы, используемые полицией, никогда не могут быть тщательно изучены судами, если информация об этой практике никогда не раскрывается в уголовных судебных делах или если ответчик не имеет финансовой возможности подать заявление в Хартию.

Хотя теоретически прокурорские и правоохранительные органы могут использовать алгоритмические технологии на многих этапах процесса уголовного правосудия – например, алгоритмические технологии оценки рисков были разработаны, приняты или рассмотрены в контексте предварительного заключения (залога), вынесения приговора, условно – досрочного освобождения и исправительных работ, [855] – рассмотрен в настоящем докладе технологии в первую очередь связаны с начальным этапом сбора информации и мониторинга работы полиции.

Сосредоточенная на локации алгоритмическая политика

[853] Приостановление судимости означает, что судимость лица исключается из национальной базы данных судимости, что потенциально может помочь человеку найти работу или возможности для получения образования без видимого шрама судимости.

[854] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 24(2).

[855] В разделе 4.2.3 ("Алгоритмические оценки рисков в системе уголовного правосудия") ниже приводится краткий обзор алгоритмических технологий оценки рисков.

Ориентированные на местоположение алгоритмические полицейские системы предназначены для определения того, где и когда может произойти потенциальная преступная деятельность. Алгоритмы, управляющие этими системами, исследуют закономерности и корреляции в исторических полицейских данных, чтобы попытаться сделать прогнозы о будущем. Затем правоохранительные органы могут принять решение о вмешательстве для сдерживания или выявления преступной деятельности, предприняв такие действия, как усиление патрулирования в целевых местах.

Полицейские службы Северной Америки уже давно используют методы, не связанные с ИИ, чтобы попытаться определить «горячие точки» преступности – географические районы, которые воспринимаются или предполагаются как имеющие относительно высокую концентрацию преступности. [856]Современные методы продолжают этот путь, используя алгоритмы для обработки больших объёмов данных и якобы выявления связей, которые в противном случае остались бы незамеченными человеческим аналитиком.

Ориентированные на местоположение технологии алгоритмической полиции могут учитывать различные переменные. Например, Prepol, один из самых известных примеров этой технологии и используемый более чем 90 полицейскими департаментами в Соединенных Штатах, [857] опирается на четыре точки данных для своего алгоритма: тип преступления, местоположение, дата и время. [858]Другие популярные алгоритмические программные системы, такие как HunchLab, [859] могут использовать дополнительные переменные, включая местоположение и тип зданий (например, школы, церкви, бары или винные магазины) и данные переписи населения. [860]Продукт моделирования местности риска, разработанный

---

[856] Council of Canadian Academies, Policing Canada in the 21st Century: New Policing for New Challenges (Ottawa, 2014) at 23-24.

[857] Caroline Haskins, «Dozens of Cities Have Secretly Experimented With Predictive Policing Software» (6 February 2019) Vice, <https://www. vice.com/en_us/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software>. В апреле 2020 года один из самых громких и давних примеров реализации PredPol, его использование Департаментом полиции Лос-Анджелеса (LAPD), был закрыт LAPD, якобы "не из-за опасений, которые вызвали активисты, а из-за финансовых ограничений из-за COVID-19, болезни, вызванной новым коронавирусом". Caroline Haskins, «The Los Angeles Police Department Says It Is Dumping A Controversial Predictive Policing Tool», BuzzFeed News (21 April 2020) <https://www.buzzfeednews.com/article/carolinehaskins1/los-angeles-police-department-dumping- predpol-predictive>.

[858] PredPol, «The Three Pillars of Predictive Policing», <https://www.predpol.com/law-enforcement>.

[859] В 2018 году HunchLab была приобретена компанией HunchSpotter, выпускающей алгоритмический инструмент обнаружения выстрелов, который ранее рассматривался (и в конечном итоге был отклонён) для принятия полицейской службой Торонто. «Shotspotter announces acquisition of HunchLab to Springboard into AI-Driven Analysis and Predictive Policing» (3 October 2018) <https://www.shotspotter.com/press-releases/shotspotter-announces-acquisition-of-hunchlab-to-springboard-into-ai-driven-analysis-and-predictive-policing/>; Jeff Gray, «Toronto police end ShotSpotter project over legal concerns», Globe and Mail (13 February 2019) <https://www.theglobeandmail.com/canada/toronto/article-toronto-police-end- shotspotter-project-over-legal-concerns/>.

[860] Leslie Kennedy, Joel Caplan & Eric Piza, «A Multi-jurisdictional Test of Risk Terrain Modeling and a Place-based

Центром общественной безопасности Университета Рутгерса, опирается на набор факторов, включая типы коммерческих учреждений, присутствующих в данном районе, и более проблемные факторы (из-за их связи с дискриминационным чрезмерным надзором за маргинальными общинами), такие как публичные призывы к «беспорядкам» и определённые типы жилья, чтобы попытаться предсказать, где могут произойти такие преступления, как угон автомобилей и насилие с применением оружия.[861]

В оставшейся части этого раздела будет представлен обзор конкретных ориентированных на местоположение алгоритмических полицейских технологий, используемых канадскими полицейскими службами, хотя данная технология может использоваться и для других возможностей, помимо алгоритмических прогнозов (например, используется только для организации данных). Раздел 4.1.1. будет обсуждаться алгоритмическая полицейская система GeoDASH, реализованная Департаментом полиции Ванкувера, и раздел 4.1.2. будет обсуждаться использование полицейской службой Торонто Environics Analytics, IBM Cognos Analytics и IBM Statistical Package for the Social Sciences software.

Департамент полиции Ванкувера: GeoDASH алгоритмические системы поддержания правопорядка

Полицейское управление Ванкувера (VPD) использует ориентированную на машинное обучение алгоритмическую систему и пользовательский интерфейс, известные как GeoDASH. GeoDASH использует исторические данные полиции, чтобы попытаться предсказать, где и когда могут произойти преступления со взломом и проникновением. В частности, алгоритмы генерируют шесть прогнозов на основе местоположения с 24-часовыми интервалами для каждого 2-часового окна между 7: 00 и 6: 59 утра следующего дня; каждый прогноз представляет собой площадь 100 квадратных метров или 500 квадратных метров.[862] Алгоритмическая полицейская система GeoDASH или «GeoDASH APS», термин, используемый для целей настоящего доклада, [863]- является первой в своём роде в Канаде, и она была создана в рамках

Evaluation of Environmental Risk-Based Patrol Deployment Strategies» (2015), Rutgers Center on Public Security, at <www.rutgerscps.org/uploads/2/7/3/7/27370595/nij6city_ resultsexecsum_final.pdf>, cited in Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 71-72.

[861] Ibid at 67-68.

[862] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019); and Matt Meuse, «Vancouver police now using machine learning to prevent property crime,» CBC (22 July 2017) <https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111>.

[863] Средство алгоритмического контроля VPD обычно связано с его приложением картирования "горячих точек" преступлений GeoDASH (Geographic Data Analysis and Statistics Hub). Однако в интервью уточнялось,

трёхстороннего частно-государственного предприятия между консорциумом академических исследователей из множества академических учреждений в Канаде и за рубежом, штатными сотрудниками VPD и Latitude Geographics. Система прошла шестимесячное исследование с 1 апреля по 30 сентября 2016 года. [864] В ходе пилотного исследования заинтересованные стороны проверили прогнозы в отношении преступлений, связанных со взломом и проникновением в жилые помещения.

После завершения пилотного проекта VPD объявила в 2017 году, что GeoDASH будет официально внедрён в качестве более широкой практики.[865]

AP GeoDASH опирается на четыре входных данных: тип преступления, географические координаты, дата и время. VPD предоставляет алгоритмам данные, возникающие исключительно из случаев, которые были вызваны жалобой гражданского лица в полицию, и исключает все сообщения, инициированные полицией (по словам констебля Райана Прокса, гражданские сообщения о преступлениях против собственности составляют примерно 90% всех данных о преступлениях против собственности).[866] Например, если полицейский был в патруле и случайно стал свидетелем кражи со взломом, этот инцидент не будет входить в обучающие данные, передаваемые алгоритмам.[867]

Цель этой политики состоит в том, чтобы уменьшить как риск, так и восприятие того, что предвзятость полиции влияет на обучающие данные или алгоритмы. [868]

После того, как система идентифицирует места повышенного риска, полицейские в форме на помеченных автомобилях назначаются для патрулирования этих районов с целью предотвращения преступной деятельности. Согласно внутреннему документу, эти группы активно ищут

что GeoDASH относится только к пользовательскому интерфейсу, который визуализирует выходы алгоритма среди прочих данных в картографическом приложении для пользователей. Лежащая в основе алгоритмическая технология не имеет названия. Интервью Райана Прокса Синтии Хоо и Йоланды Сонг (7 мая 2019). Для удобства в данном отчете рассматривается вся система алгоритмического контроля (алгоритмическая технология в сочетании с интерфейсом GeoDASH, облегчающим ее использование) как система алгоритмического контроля GeoDASH ("GeoDASH APS"). "GeoDASH" будет зарезервирован, чтобы ссылаться только на пользовательский интерфейс, к которому VPD может добавить множество программных приложений, только одно из которых является прогнозирующей технологией управления.

[864] Vancouver Police Department, «Vancouver Police adopt new technology to predict property crime» (21 July 2017) <https://mediareleases. vpd.ca/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/>.

[865] Vancouver Police Department, «Vancouver Police adopt new technology to predict property crime» (21 July 2017) <https://mediareleases. vpd.ca/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/>

[866] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

[867] Ibid.

[868] «Я не хотел иметь никаких данных, которые могли бы быть восприняты как предвзятое отношение полиции с точки зрения генерации звонков. [...] Я верю, правда это или нет, что [предвзятые представления о преступности, предрасполагающие полицию к развертыванию в определенных районах, приводящие к потенциальному самосбывающемуся пророчеству] происходят в полиции Ванкувера, я не хотел, чтобы призрак, который может даже войти в предвзятость данных. Исходя из этого, я принял решение, что мы будем использовать только публичные сообщения об имущественных преступлениях.» Ibid.

«подозрительную активность во время своего патрулирования и будут участвовать в упреждающих действиях, таких как мониторинг переулков и выявление потенциальных POI [лиц, представляющих интерес]/известных правонарушителей, въезжающих в этот район»[869] VPD может также уведомить гражданские квартальные блок-посты в прогнозируемых жилых районах и попросить их проявлять дополнительную бдительность в своих районах в течение соответствующих периодов времени. [870]

По словам Prox, команда прогнозной полиции в VPD находится под сильным влиянием общего регламента защиты данных (GDPR) и европейского закона о конфиденциальности и с осторожностью относится к развитию прогнозной полиции в Соединенных Штатах. [871] Таким образом, VPD активно принимает меры по смягчению потенциального вреда и дискриминации со стороны AP GeoDASH. Уникальной особенностью программы VPD является использование «исключительных зон», которые учитывают «чувствительные районы» города, вызывающие чрезмерные проблемы с полицией, такие как район Даунтаун Истсайд (DTES). Если какое-либо из прогнозируемых мест повышенного риска попадает в исключительную зону, оно автоматически заменяется местом, которое идентифицировано как имеющее следующий самый высокий риск взлома и входа в систему. В результате прогностическая система не направляет сотрудников в указанные зоны, даже если они изначально определены алгоритмами как «зоны повышенного риска».

В настоящее время DTES является единственной исключительной зоной, которую определил VPD, и она была отмечена как таковая с самого начала инициативы.[872] VPD также отслеживает потенциальную чрезмерную полицейскую деятельность, возникающую в результате использования GeoDASH APS в других общинах, отслеживая и контролируя, как часто GeoDASH APS направляет сотрудников в любой данный район города Ванкувера, уделяя особое внимание любым районам, считающимся «социально-экономическими или культурно чувствительными» (одним из примеров является район южного склона в Ванкувере, где проживает большая Индо-канадская община).[873] На момент написания этой статьи VPD не определила, что они обнаружили чрезмерную представленность конкретных районов в какой-либо из прогнозируемых областей, и поэтому не добавила никаких дополнительных исключающих зон. [874]

---

[869] Vancouver Police Department, «Predictive Policing» (obtained through freedom of information request 18-3224A_2).
[870] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).
[871] Ibid.
[872] Ibid.
[873] Ibid.
[874] Ibid.

Кроме того, чтобы оставаться бдительным к возможности алгоритмически чрезмерного контроля за другими сообществами, VPD полагается на совещания, проводимые каждые 3-4 месяца между подразделением прогнозной полиции и подразделением служб общественной полиции.[875]На этих встречах последние могли бы общаться, если бы существовали заинтересованные или подверженные риску сообщества, не находящиеся на радаре первых.[876] Одним из примеров является появление инициатив в области социального жилья в Южном Ванкувере. VPD работал с городом Ванкувер, чтобы определить местоположение этих инициатив и связанных с ними информационно – пропагандистских программ, а затем контролировал чрезмерную представленность этих районов в прогнозах GeoDASH APS (и не обнаружил никакой чрезмерной представленности на момент интервью).[877]

Ещё одна область, вызывающая озабоченность при использовании GeoDASH APS, — это основанные на местоположении полицейские остановки и задержания. Что касается опасности алгоритмизированных полицейских остановок и задержаний, то Prox заявил, «с точки зрения обучения мы очень чётко даём понять, что, если полицейские развёрнуты в прогнозируемых местах, вы не можете использовать систему прогнозирования в качестве основания для проверки улиц». [878]VPD попыталась измерить во время пилотного исследования прогностической полиции, происходит ли больше уличных проверок в прогнозируемых ящиках GeoDASH APS по сравнению с местоположениями, которые не были внутри ящиков. Однако, по словам Prox, не было достаточно данных для поддержки каких-либо значимых показателей из-за низкого общего числа проверок улиц в прогнозируемых местах в целом.[879]

[875] Ibid.
[876] Ibid.
[877] Ibid.
[878] Ibid.
[879] Ibid.

Полицейская служба Торонто: Environics Analytics и программное обеспечение IBM «Crime Insight and Prevention»

Есть признаки того, что полицейская служба Торонто (TPS), возможно, рассматривает или заинтересована в разработке ориентированной на местоположение алгоритмической программы в будущем. По крайней мере с 2016 года TPS сотрудничает с Environics Analytics. Environics Analytics – это фирма, которая в первую очередь предоставляет услуги анализа данных для деловых и маркетинговых целей, [880]чтобы «исследовать использование данных и технологий в более оптимальном соотношении полицейских ресурсов и преступности». [881] В 2018 году старший вице-президент Environics Analytics написал, что одной из целей сотрудничества является разработка алгоритмических моделей, которые идентифицируют зоны с высоким уровнем преступности.[882] По словам Ричарда Буара, такие факторы, как уровень преступности за предыдущий год, возраст, доход и типы жилья в данной географической области, используются для прогнозирования уровня преступности в этой области.[883] Алгоритмическая модель информирует о количестве офицеров, которых TPS назначает в район в течение следующих 12 месяцев.[884] Однако в интервью представитель правоохранительных органов Канады подтвердил, что TPS в настоящее время не занимается алгоритмически управляемой прогностической полицией. Представитель также заявил, что TPS помнит о связанных с этим вопросах и не намерена немедленно внедрять такую технологию и, насколько им известно, не взаимодействовала с поставщиками с этой целью. Представитель действительно указал, что TPS заинтересована в использовании данных для принятия решений по вопросам общественной безопасности, таким как насилие с применением огнестрельного оружия и имущественные преступления.[885]

Помимо Environics, TPS имеет доступ к программному обеспечению IBM Cognos Analytics и SPSS (Statistical Package for the Social Sciences).[886] Обе эти программы являются частью решения IBM «Crime Insight and Prevention solution», которое использует интеллектуальный анализ данных и

---

[880] Environics Analytics, «How we help», <https://www.environicsanalytics.com/en-ca/how-we-help>. Он предлагает ряд собственных баз данных, включая базу данных под названием CriminStats, которая использует статистику, демографические данные и компьютерное моделирование для определения вероятности совершения преступлений в любом месте в Канаде, США и Великобритании.

[881] Richard Boire, «Data-Driven Decisions for Law Enforcement in Toronto» (17 August 2018) Predictive Analytics Times, <https://www.predictiveanalyticsworld.com/patimes/data-driven-decisions-for-law-enforcement-in-toronto/9640/>.

[882] Ibid.

[883] Ibid.

[884] Ibid.

[885] Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).

[886] Ibid.

ориентированное на местоположение прогнозное моделирование. IBM заявляет, что эти инструменты позволят правоохранительным органам «предвидеть инциденты, выявлять преступления и преступников, повышать уровень раскрываемости преступлений и оптимизировать использование ресурсов». [887]Cognos – это инструмент анализа данных, который использует ИИ и машинное обучение для обнаружения паттернов и перевода анализа данных на простой язык. [888] SPSS предлагает расширенные функции статистического анализа и алгоритмической аналитики.[889] В то время как эти программы предлагают алгоритмически управляемые возможности предсказательной полиции, TPS заявила, что она не использует их для предсказательных целей; вместо этого они используют их для отчётности и статистической информации. [890] По словам опрошенного представителя правоохранительных органов, полного использования возможностей этих программ для алгоритмов и автоматизации не существует, по крайней мере частично из-за ограниченности ресурсов службы.[891] TPS также заявила, что для рассмотрения вопроса о реализации прогностической полицейской программы потребуется согласование с провинциальными и/или федеральными стратегиями управления.[892]

Личностно-ориентированная алгоритмическая политика

Ориентированные на человека алгоритмические полицейские системы якобы предназначены для выявления лиц, которые могут быть вовлечены в будущую преступную деятельность, или они предназначены для оценки того, какой уровень риска имеет конкретный человек для участия или быть жертвой будущей преступной деятельности. Такие алгоритмические оценки не основываются главным образом на факторах окружающей среды или географических данных о преступности, как в случае ориентированной на местоположение полиции; вместо этого они обрабатывают личные данные, такие как информация о семье, друзьях или сообщниках; их активность в социальных сетях; судимости или появление в других полицейских базах данных, которые связаны с конкретным человеком. [893] Эти факторы используются в качестве входных данных для ориентированного на человека

---

[887] IBM Software Group, «Crime prediction and prevention: A safer public through advanced analytics» (June 2010) IBM Software Group White Paper, 4.
[888] IBM, «IBM Cognos Analytics», <https://www.ibm.com/ca-en/marketplace/business-intelligence>.
[889] IBM, «IBM SPSS software», <https://www.ibm.com/analytics/spss-statistics-software>.
[890] Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).
[891] Ibid.
[892] Ibid.
[893] Andrew G Ferguson, «Policing Predictive Policing» (2017) 94:5 Washington University Law Review 1109 at 1137-42.

алгоритмического инструмента контроля, который затем предоставляет выходные данные «оценки риска» для данного человека. Оценка риска предназначена для отражения прогнозируемой вероятности того, что данное лицо совершит или будет вовлечено в преступную деятельность в будущем или в течение определённого периода времени. [894]

Правоохранительные органы могут действовать в соответствии с этими алгоритмическими прогнозами различными способами, в том числе нацеливаться на выявленных лиц для усиления контроля или вступать в контакт с выявленными лицами якобы для того, чтобы удержать их от любой преступной деятельности, которую алгоритм предсказал, что они могут участвовать – независимо от того, действительно ли этот человек собирался участвовать в преступной деятельности. В тех случаях, когда человек, по прогнозам, подвергается риску вовлечения в преступную деятельность или причинения вреда в результате преступной деятельности, но не обязательно совершает её, полицейские службы могут вместо этого связать его с социальными службами. Результатом применения ориентированных на человека алгоритмических полицейских систем является то, что люди потенциально вступают в контакт с системой уголовного правосудия на основе неточной, ненадёжной или предвзятой технологии. Например, полицейские службы могут полагаться на алгоритмические предсказания, чтобы вмешиваться в право человека на частную жизнь или свободу, но у человека мало или вообще нет гарантий, чтобы предотвратить нарушение его конституционных или человеческих прав.[895]

Ориентированные на человека алгоритмические полицейские системы в различных городах США существуют уже много лет и используют различные методы анализа данных. Например, начиная с 2012 года Департамент полиции Чикаго (CPD) вел список стратегических субъектов (SSL, в просторечии называемый «тепловым списком») лиц, которые якобы подвергались риску стать преступником или жертвой насилия с применением огнестрельного оружия.[896]В «тепловом списке» использовался алгоритм, который изучал 11 переменных, которые, как сообщается, включали предыдущую криминальную

---

[894]Смотрите, например, "Отображаемая информация представляет собой отождествленный список данных об аресте с 1 августа 2012 года по 31 июля 2016 года, который используется алгоритмом стратегического субъекта департамента полиции Чикаго... создать оценку риска, известную как Стратегический список тем или "SSL". Эти оценки отражают вероятность участия человека в инциденте со стрельбой либо в качестве жертвы, либо в качестве правонарушителя. Баллы рассчитываются и ставятся по шкале от 0 (чрезвычайно низкий риск) до 500 (чрезвычайно высокий риск). На основе версии Стратегического алгоритма субъекта, основанной на этих временных рамках, лица с судимостью ранжируются по восьми признакам, не включая расу или пол. «Strategic Subject List» (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>.

[895] Эти вопросы будут более подробно освещены в части 5 ("Международные последствия алгоритмической работы полиции для прав человека и Хартии") доклада.

[896] Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 46.

историю, статус условно-досрочного освобождения и полицейские записи о предполагаемом членстве в банде;[897]данные об аресте, которые были использованы CPD для создания оценок риска SSL, были предоставлены на общедоступном портале данных.[898] В январе 2020 года CPD прекратил использование программы по причинам, включавшим в себя недостаточную надёжность модели. [899]

В Новом Орлеане полицейское управление использовало программное обеспечение, разработанное компанией Palantir Technologies, для выявления лиц, подвергающихся риску стать преступниками или жертвами насилия, путём анализа их ассоциаций с использованием метода, известного как анализ социальных сетей (SNA).[900] Программное обеспечение Palantir интегрировало отдельные городские базы данных в единые системы и выявило скрытые связи в данных, хранящихся в этих базах данных.[901]

Некоторые правоохранительные органы Канады выразили меньший энтузиазм в отношении личностно-ориентированных подходов к алгоритмической полицейской деятельности по сравнению с ориентированными на местоположение подходами. констебль Райан Прокс из VPD заявил, что индивидуальное прогнозирование преступной деятельности является «слишком высоким риском» и что «с этической точки зрения было бы предосудительно двигаться в этом направлении.» [902]Прокс особенно интересовался ориентированными на человека прогностическими полицейскими программами, наблюдаемыми в Лос-Анджелесе, Новом Орлеане и Чикаго, делая следующее наблюдение относительно их потенциального воздействия на затронутые общины в Соединенных Штатах: «если у вас есть этнически предвзятый алгоритм, затем вы можете преобразовать сообщество в полицейское государство, где у вас есть такая чрезмерная представленность полицейских ресурсов в очень ограниченной геопространственной области, что

---

[897] Ibid at 46-49. As noted in Section 2.2 («Bias and Inaccuracies in Police Data») of this report, factors such as «gang membership» can be highly discretionary and prone to error and discriminatory bias.

[898] «Strategic Subject List» (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki- r3np>. Another well-known predictive policing program that was later shut down, Operation LASER, by the Los Angeles Police Department, is discussed below in Section 4.2.1 («Calgary Police Service: Palantir Gotham and IBM i2 Analyst Notebook»).

[899] Sam Charles, «CPD decommissions 'Strategic Subject List'«, Chicago Sun Times (27 January 2020), <https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson>.

[900] Анализ социальных сетей (CHC) "основан на посылке о том, что отношения между отдельными лицами могут информировать и даже прогнозировать поведение человека", и используется в полиции для "анализа возможностей преступных сетей, того, как такие сети влияют на преступную деятельность, и распространения насильственных преступлений внутри сообщества или среди населения". See Andrew Papachristos & Michael Sierra-Arevalo, «Policing the Connected World» (2018) Office of Community Oriented Policing Services, at viii <https://cops.usdoj.gov/RIC/Publications/cops-w0859-pub.pdf>. SNA in Canada is discussed below in Section 4.3 («Algorithmic Surveillance Tools»).

[901] Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 49-51.

[902] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

чрезмерная представленность полицейских ресурсов может превратить сообщество в почти как в осаде».[903]

В оставшейся части этого раздела будет представлен обзор конкретных ориентированных на человека алгоритмических полицейских технологий, используемых, разрабатываемых или имеющихся в распоряжении канадских полицейских служб. В разделе 4.2.1. обсуждается использование полицейской службой Калгари программного обеспечения Palantir Technologies и IBM I2 Analyst Notebook, последний из которых используется для алгоритмического анализа социальных сетей. В разделе 4.2.2 будет обсуждаться технология алгоритмической полицейской деятельности, разрабатываемая в лаборатории прогнозной аналитики полиции Саскачевана (SPPAL). В разделе 4.2.3 будет кратко отмечено использование алгоритмических инструментов оценки рисков на других этапах системы уголовного правосудия, включая освобождение под залог, вынесение приговора и условно-досрочное освобождение.

Полицейская служба Калгари: Palantir Gotham и IBM I2 Analyst Notebook

В конце 2012 года полицейская служба Калгари (CPS) приобрела лицензию на программное обеспечение у компании Palantir Technologies за 1,4 миллиона долларов.[904] В настоящее время CPS использует версию продукта Palantir Gotham 2018 года[905] для интеграции различных внутренних источников данных в единую систему доступа к данным и их анализа. [906]

Документы, подготовленные Palantir и CPS, указывают на то, что информация из открытых источников (например, общедоступные социальные сети и другой онлайн-контент), электронная почта и телекоммуникационная информация, а также коммерческая информация третьих лиц (например, финансовые отчёты и кредитная история) также могут быть включены в систему.[907] Однако сотрудник правоохранительных органов в Калгари сообщил, что CPS использует Palantir для интеграции определённых внутренних файлов, данных о диспетчерских вызовах и своей нишевой системы управления записями (RMS). Нишевая система содержит некоторые из ранее

---

[903] Ibid.
[904] City of Calgary, «Purchase Order» (obtained through freedom of information request 2018-G-0203).
[905] Calgary Police Service, «Transition from Palantir 2012 to PG2018» (obtained through freedom of information request 18-G-0814).
[906] Calgary Police Service, «Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft» at 9, (obtained through freedom of information request 18-G-1921).
[907] Ibid at 15, 47; Palantir, «Palantir Platform Capabilities Brief» (11 October 2012), presentation to Calgary Police Service (obtained through freedom of information request 18-G-1921).

изолированных источников данных полицейской службы Калгари (CPS's), такие как информация о частых правонарушителях. [908]

Согласно записям CPS, которые были выпущены по запросу FOI, Palantir Gotham позволяет авторизованным пользователям CPS осуществлять поиск по интегрированным данным для обнаружения и визуализации ассоциаций между отдельными лицами, организациями, местоположениями, полицейскими отчётами об инцидентах, проверками (аналогичными данным проверки улиц или кардинга), недвижимостью и транспортными средствами.[909] Ассоциации и связи, создаваемые Palantir, используются для информирования офицеров и аналитиков о понимании отношений и поведения отдельных лиц. [910]

Согласно проекту оценки воздействия на частную жизнь (PIA), проведённых CPS в 2014 году, информация о физических характеристиках, взаимоотношениях, взаимодействии с полицией и «возможной вовлечённой деятельности» (открытая и неопределённая категория входных данных) хранится для всех лиц, взаимодействующих с полицией, включая жертв и свидетелей. Для лиц, подозреваемых в совершении преступления, собираются дополнительные данные, такие как данные об их религиозной принадлежности. [911] CPS также использует Palantir, чтобы определить, где происходят преступления и вызовы на обслуживание. [912]

CPS признал в своём проекте PIA, что оценки с использованием системы Palantir могут привести к ложным ассоциациям между невиновными лицами и преступными организациями и подозреваемыми. [913]В проекте PIA предлагались меры, направленные на снижение таких рисков, включая установление правил ввода данных, использование аудиторских возможностей программного обеспечения, позволяющих отслеживать изменения, вносимые в данные, и использование функции моделирования данных, которая якобы позволяет аналитикам избегать создания неверных ассоциаций.[914] По крайней мере один важный элемент системы подотчётности, изложенной в проекте PIA, – орган управления платформой Palantir – в настоящее время не функционирует.[915]

Орган управления платформой Palantir должен был отвечать за надзор за процессами обеспечения качества данных, внедрение новых функций и

---

[908] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).
[909] Calgary Police Service, «Transition from Palantir 2012 to PG2018» (obtained through freedom of information request 18-G-0814).
[910] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).
[911] Calgary Police Service, «Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft» at 29-30, (obtained through freedom of information request 18-G-1921).
[912] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).
[913] Calgary Police Service, «Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft» at 35, (obtained through freedom of information request 18-G-1921).
[914] Ibid.
[915] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

источников данных для системы Palantir, а также периодический обзор последствий для конфиденциальности.[916] По словам одного из сотрудников правоохранительных органов в Калгари, существует рабочая группа по управлению информацией для рассмотрения предлагаемых изменений в любой из систем агентства, включая последствия таких изменений для управления данными, а руководящий комитет по управлению информацией осуществляет надзор за деятельностью рабочей группы в целях обеспечения стратегического руководства и надзора. [917] Однако CPS не раскрыл никаких окончательных или формализованных политик, или руководящих принципов использования программного обеспечения Palantir в ответ на запрос FOI, направленный для получения информации об использовании ими систем Palantir.

Там, где технология Palantir была развернута в Соединенных Штатах, программное обеспечение использовалось для содействия громким и спорным инициативам. В Лос-Анджелесе, в рамках Лос-Анджелесской стратегической программы извлечения и восстановления Лос-Анджелеса («Операция Лазер»), технология Palantir, как сообщается, использовалась для интеграции и анализа данных из различных местных, общегосударственных и национальных правоохранительных источников, а также данных, не относящихся к правоохранительным органам, о социальных услугах, медицинских услугах, выкупе прав выкупа, социальных сетях, коммунальных платежах и даже телефонных записях сетей пиццерий. [918] Полученные выводы используются для определения зон, которые прогнозируют горячие точки для преступлений, связанных с оружием. Лица, считающиеся «хроническими правонарушителями», также преследуются с целью отслеживания их передвижения и деятельности, уведомления преследуемого лица о том, что за ними ведётся наблюдение в попытке сдержать потенциальную преступную деятельность, или удаления этого лица из района или района.[919] Эти программы были встречены значительной реакцией общественности и оппозиции,[920] а также критикой со стороны генерального инспектора Департамента полиции Лос-Анджелеса (LAPD), офис которого выявил серьёзные проблемы с практикой сбора данных и механизмами надзора LAPD.[921] Генеральный

---

[916] Calgary Police Service, «Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft» at 20, (obtained through freedom of information request 18-G-1921).

[917] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

[918] Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017) at 9, 99-100; Mark Smith, «Review of Selected Los Angeles Police Department Data-Driven Policing Strategies» (12 March 2019) Los Angeles Police Commission Inspector General, at 5 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

[919] Mark Smith, «Review of Selected Los Angeles Police Department Data-Driven Policing Strategies» (12 March 2019) Los Angeles Police Commission Inspector General, at 5-9 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

[920] Stop LAPD Spying Coalition, «Before the Bullet Hits the Body: Dismantling Predictive Policing in Los Angeles» (8 May 2018), <https:// stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf>.

[921] Mark Smith, «Review of Selected Los Angeles Police Department Data-Driven Policing Strategies» (12 March

инспектор рекомендовал сократить программу, ограничив широкие полномочия полиции в отношении обозначения отдельных лиц в качестве хронических правонарушителей, и что программа должна в целом подлежать ряду механизмов надзора прозрачности и надлежащей правовой процедуры. [922] Полиция Лос-Анджелеса закрыла операцию лазер в апреле 2019 года, после совещания, на котором» члены полиции применяли методы. [923]

Как отмечалось выше, CPS в настоящее время не использует технологию Palantir для своих алгоритмических полицейских возможностей, таких как те, на которые полагалась полиция Лос-Анджелеса. CPS полагается на программное обеспечение Palantir, чтобы интегрировать и организовать данные, а не делать из них алгоритмические выводы или прогнозы. Однако это не обязательно означает, что CPS никогда не начнёт использовать функции алгоритмической полиции Palantir в будущем.

Кроме того, CPS действительно занимается алгоритмическим анализом социальных сетей, используя комбинацию Palantir и IBM I2 Analyst Notebook. Palantir используется для связи и построения сетей, которые рисуют отношения между данными в собственных базах данных CPS, таких как данные, хранящиеся в системе управления записями ниши. В частности, в Palantir «личностисвязаны друг с другом на основе события, которое произошло или было зарегистрировано в системе CPS». Реляционная сеть, построенная в Palantir, затем импортируется в IBM I2 Analyst Notebook, который содержит встроенный инструмент анализа социальных сетей. Этот инструмент ранжирует центральные акторы и ключевые игроки в рамках конкретной социальной сети, основываясь на таких показателях, как «между собой, близость, степень и собственный вектор (концентратор и авторитет) меры центральности».[924]

Недавние сообщения свидетельствуют о том, что Palantir стремится расширить использование своей технологии в Канаде в целом, что может увеличить использование её алгоритмических полицейских возможностей правоохранительными органами по всей стране. В августе 2019 года бывший посол Канады в Соединенных Штатах Дэвид Макнотон подал в отставку со своего поста посла, чтобы быть назначенным главой канадских операций Palantir из штаб-квартиры, базирующейся в Оттаве.[925] Затем Макнотон объявил в апреле 2020 года, что Palantir ведёт диалог с федеральным правительством и

2019) Los Angeles Police Commission Inspector General, at 5-9 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

[922] Ibid.

[923] Mark Puente, «LAPD ends another data-driven crime program touted to target violent offenders», (12 April 2019) Los Angeles Times, https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html>.

[924] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019); and Pak Chung Wong, et al, «Visual Matrix Clustering of Social Networks» (2013) 33:4 IEEE Computer Graphics and Applications 88 at 90.

[925] Justin Ling, «Palantir's big push into Canada,» OpenCanada.org, Centre for International Governance Innovation (25 October 2019), <https:// www.opencanada.org/features/palantirs-big-push-into-canada/>.

правительствами Онтарио, Альберты и Британской Колумбии относительно их мер реагирования на пандемию COVID-19.[926]

Решение Palantir расширить свою деятельность в Оттаве может быть частично обусловлено канадскими законами о конфиденциальности, которые снижают способность компании привлекать канадские правоохранительные органы в качестве клиентов при работе за пределами Соединённых Штатов. Вообще говоря, правоохранительные органы связаны законодательством о неприкосновенности частной жизни и обязательствами по защите частной жизни в соответствии с Уставом, которые ограничивают обстоятельства, при которых правоохранительным органам разрешается передавать или хранить персональные данные физического лица экстерриториально.[927] Технология Palantir может потребовать обмена данными с компанией для выполнения определённых функций. В контракте с городом Новый Орлеан должен был предоставить Palantir доступ ко всем «источникам данных и записей», которые хотел проанализировать в «интегрированной аналитической среде Palantir».[928]

Учитывая, что Palantir может потребовать от своих клиентов предоставить компании прямой доступ к любым данным, подлежащим алгоритмическому анализу, расширение операций Palantir внутри границ Канады может быть попыткой обеспечить или стимулировать более широкое внедрение своих технологий среди правоохранительных органов Канады, снижая риск нарушения законов о локализации данных.

---

[926] Murad Hemmadi, «Palantir's MacNaughton says data-mining firm is working with Ottawa, three provinces on COVID-19,» The Logic (30 April 2020), <https://thelogic.co/news/exclusive/palantirs-macnaughton-says-data-mining-firm-is-working-with-ottawa-three-provinces-on- covid-19/>.

[927] Wakeling v Соединенные Штаты Америки, 2014 SCC 72. Некоторые провинции несут обязательства по локализации данных, применимые к государственным учреждениям (Закон о свободе информации и защите частной жизни, RSBC 1996, c 165, s 30.1; Закон о международной защите личной информации, SNS 2006, c 3, ss 9 (2) d), 9 (3) b), или другие препятствия на пути раскрытия частных данных за пределами границ Канады. Например, законодательство Альберты о конфиденциальности, применимое к государственным учреждениям, таким как CPS (Закон о свободе информации и защите частной жизни), как представляется, вообще не разрешает разглашение данных правоохранительными органами частным компаниям, а статья 40 Закона разрешает разглашение информации правоохранительным органам в иностранных государствах только "в соответствии с договоренностью, письменным соглашением, договором или законодательным органом".

[928] «License and Services Agreement,» entered into as of February 23, 2012 by Palantir Technologies Inc. and the City of New Orleans, <https:// www.documentcloud.org/documents/4344821-K12-168-Palantir-Technologies.html>.

Лаборатория прогнозной аналитики полиции Саскачевана (SPPAL)

В ноябре 2015 года полицейская служба Саскатуна (SPS) в партнёрстве с Университетом Саскачевана и Правительством Саскачевана создала лабораторию прогнозной аналитики полиции Саскачевана (SPPAL), которая находится в штаб-квартире.[929] SPPAL предназначен для решения ряда проблем преступности и общественной безопасности, начиная с проекта, ориентированного на пропавших без вести лиц. Изучая факторы риска и модели поведения пропавшей молодёжи в Саскачеване, SPPAL разрабатывает предварительную алгоритмическую модель для выявления детей и молодёжи, которым грозит опасность пропасть без вести. [930]После внедрения эта модель будет передана партнёрам по социальному обслуживанию, хотя в некоторых случаях она уже была передана для целей тестирования.[931]

SPPAL работает с данными муниципальной полиции только из SPS, насколько известно авторам по состоянию на 14 февраля 2020 года, хотя соглашение с Ассоциацией начальников полиции Саскачевана предоставит лаборатории прогнозной аналитики доступ к данным всех муниципальных полицейских служб провинции и данным отдела RCMP «F» Division.[932]SPPAL также выразил своё намерение в конечном итоге включить данные социальных сетей в обучение и разработку своих моделей. [933] Интервью с представителем SPPAL ясно сказано, что проект всё ещё находится на ранней стадии и что SPPAL рассматривает множество вариантов управления данными и обмена ими с муниципальными полицейскими учреждениями, уделяя особое внимание возможностям безопасности, таким как сохранение собранных данных конфиденциальными и зашифрованными.[934]

---

[929] Meaghan Craig, «Saskatoon police lead the country with Predictive Analytics Lab» (15 January 2016) Global News <https://globalnews.ca/ news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/>. В частности, представитель SPPAL пояснил, что проект находится в SPS благодаря тому, что это учреждение уже располагает инфраструктурой и институциональными ресурсами для обеспечения необходимого уровня безопасности и удовлетворения других технических и организационных потребностей. Дополнительные причины заключались в том, что полиция, как правило, является департаментом, который принимает звонки пропавших без вести - в центре внимания инаугурационного проекта SPPAL - и в привлечении офицеров, которые уже дали присягу. Однако представитель предположил, что при наличии достаточного финансирования, ресурсов и инфраструктуры такой проект, как Лаборатория прогнозной аналитики, можно было бы в равной степени учредить в качестве "Лаборатории решений для общин", независимой от полицейских служб. Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

[930] Amelia Thatcher, «Stopping crime - by the numbers» (3 October 2016) 78:2 Gazette <http://www.rcmp-grc.gc.ca/en/gazette/stopping- crime-the-numbers>.

[931] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019). В этих случаях алгоритмическая модель SPPAL была передана агентствам социального обслуживания, которые проверили модель на собственных данных и предоставили SPPAL обратную связь. Это не позволяло на данном этапе передавать данные социальных служб в SPPAL или SPS для целей тестирования.

[932] Ibid.

[933] Ibid.

[934] Ibid.

Работа, которой занимается SPPAL, была описана как расширение «хабовой модели» отслеживания рисков. [935] Эта модель предполагает систематический обмен информацией между учреждениями социального обслуживания и правоохранительными органами в целях мониторинга и выявления отдельных лиц или общин, которые считаются маргинализированными и подверженными риску. [936] Одна из ключевых целей SPPAL состоит в том, чтобы предсказать риск и вмешаться на более ранней стадии в жизни человека, прежде чем он достигнет точки, где кто-то принесёт своё дело в программу хаба.[937] Представитель SPPAL сообщил, что после развёртывания алгоритмическая модель пропавших без вести лиц будет оценена с использованием методов, разработанных партнёрами из Университета Саскачевана.[938]

Нынешний проект SPPAL уникален тем, что он претендует на то, чтобы сосредоточиться на упреждающем выявлении потенциальных жертв или тех, кто может причинить вред себе.

Эти оценки проводятся с использованием анализа рисков/потребностей и стратегий профилактики, а не прогнозирования потенциальных преступников, как это было в случае с личностно-ориентированными алгоритмическими полицейскими программами в Чикаго, Новом Орлеане и Лос-Анджелесе. Однако SPPAL намеревается расширить сферу своей алгоритмической работы для решения других проблем безопасности и общественных проблем, таких как повторные и насильственные правонарушители, насилие в семье, опиоидный кризис и лица с психическими заболеваниями, вступившие в конфликт с системой уголовного правосудия. [939]По словам представителя SPPAL, который был опрошен для этого отчёта, «мы выбираем сложные проблемы, где мы чувствуем, что можем повлиять на людей, которые уязвимы, чтобы помочь им быть в безопасности, помогая нашим сообществам быть в безопасности».[940]

---

[935] Объяснение модели концентратора в отношении алгоритмической политики см. в документе IN FOCUS # 3: The Hub Model of Community Safety.

[936] Abeba Taddese, «Saskatchewan, Canada: The Hub Model for Community Safety» Results for America, <http://results4america.org/wp- content/uploads/2017/07/LandscapeCS_Canada_4.pdf>; Nathan Munn, «Police in Canada Are Tracking people's 'Negative' Behavior In a 'Risk' Database» (27 February 2019) Vice <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a- risk-database>.

[937] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

[938] Ibid.

[939] «Saskatoon police analytics lab will try to predict crime before it happens,» CBC News (14 January 2016) <https://www.cbc.ca/news/ canada/saskatoon/saskatoon-police-analytics-lab-will-try-to-predict-crime-before-it-happens-1.3403632>; Meaghan Craig, «Saskatoon police lead the country with Predictive Analytics Lab» (15 January 2016) Global News <https://globalnews.ca/news/2455063/saskatoon-police-lead-the- country-with-predictive-analytics-lab/>; Interview.

[940] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

Алгоритмическая оценка рисков в системе уголовного правосудия

Многие ориентированные на человека технологии алгоритмического контроля принимают форму алгоритмических оценок рисков. Такие оценки предполагают вычисление уровня мнимого риска человека, например, подвержен ли он высокому или низкому риску насилия или повторного преступления. Например, в Соединённом Королевстве полиция Дарема использует инструмент оценки риска причинения вреда (HART) для прогнозирования того, подвергаются ли задержанные лица низкому, умеренному или высокому риску совершения правонарушения в течение двухлетнего периода. Это предсказание затем используется для того, чтобы повлиять на решение должностных лиц о возбуждении уголовного преследования путём предъявления обвинений против данного лица или же вместо этого направить его в диверсионную схему, включающую программу реабилитации во внесудебном порядке.

Модель HART учитывает факторы, связанные с оскорбительным поведением индивида, а также возраст, пол, почтовый индекс и данные разведки.[941]

Ориентированные на человека алгоритмические оценки рисков могут также использоваться в других областях системы уголовного правосудия. Хотя в настоящем докладе особое внимание уделяется полицейскому контексту, важно отметить, что алгоритмические системы прогнозирования используются на этапах предварительного производства (залог), вынесения приговора и исправления в системе уголовного правосудия.[942]

---

[941] Hannah Couchman, «Policing by Machine: Predictive policing and the threat to our rights,» (January 2019) Liberty,at 50-51 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>. Этот инструмент получил критику за рассмотрение данных почтовых индексов, которые могут выступать в качестве доверенных лиц по расовым мотивам и тем самым приводить к дискриминационным по расовому признаку результатам. Смотри также Мэтт Берджесс, "полиция Великобритании использует ИИ для информирования о решениях о содержании под стражей - но это может быть дискриминацией в отношении бедных". See also Matt Burgess, «UK police are using AI to inform custodial decisions - but it could be discriminating against the poor», (1 March 2018) Wired <https://www.wired. co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>.

[942] See e.g., Tom Simonite, «Algorithms Were Supposed to Fix the Bail System. They Haven't,» Wired (19 February 2020) <https://www.wired. com/story/algorithms-supposed-fix-bail-system-they-havent/>; Ashley Mullen, «Incarceration or E-Carceration: California's SB 20 Bail Reform and the Potential Pitfalls for Pretrial Detainees» (2018) 104 Cornell Law Review 1867; Alicia Solow-Niederman, YooJung Choi & Guy Van den Broeck, «The Institutional Life of Algorithmic Risk Assessment» (2019) 34 Berkeley Technology Law Journal 705; and Carolyn McKay, «Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decision-making» (2020) 32:1 Current Issues in Criminal Justice 22.

Каково определение понятия «подверженный риску» и как мы обозначаем людей, которые подвергаются риску, и какое определение идеализированного гражданина мы оперируем? – Центр судебных исков чернокожего населения[943]

Алгоритмические инструменты оценки рисков используются на всей территории Соединённых Штатов в досудебных разбирательствах, связанных с залогом, и в послесудебных разбирательствах, связанных с вынесением приговора и условно-досрочным освобождением. Канадские исследователи, правительственные учреждения и начинающие компании также начали рассматривать алгоритмические инструменты оценки рисков в залоге.[944] Инструмент «профилирование управления исправительными учреждениями для альтернативных санкций» (COMPAS) широко используется в Соединённых Штатах для оценки риска повторного правонарушения обвиняемого в целях информирования о предварительном заключении, вынесении приговора и решениях об условно-досрочном освобождении. [945] Алгоритм(ы), лежащий в основе COMPAS, является собственностью компании и не раскрывается обвиняемым или их адвокатам. Как сообщается, он составлен из 137 вопросов, на которые отвечает обвиняемый или которые взяты из полицейских данных. [946]Опрос включает в себя вопросы о судимости и поведении семьи и друзей обвиняемого, а также вопросы, связанные с уровнем образования и занятости обвиняемого.[947]

Многочисленные исследования в Саскачеване изучали алгоритмические методы оценки досудебного риска в отношении предварительного заключения и вынесения приговоров, причём исследователи отмечали, что в канадском

---

[943] Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

[944] See e.g., Alyshah Hasham, «Soon, intelligent machines could help decide whether to keep people in jail. It's time to prepare,» Toronto Star (19 July 2019) <https://www.thestar.com/news/gta/2019/07/19/soon-intelligent-machines-could-help-decide-whether-to-keep-people-in-jail-its- time-to-prepare.html>; and Agnese Smith, «Automating Justice» (13 March 2018) CBA National, <https://nationalmagazine.ca/en-ca/articles/law/ ethics/2018/automating-justice>.

[945] Julia Angwin et al., «Machine Bias» (23 May 2016) ProPublica, <https://www.propublica.org/article/machine-bias-risk-assessments-in- criminal-sentencing>.

[946] Ibid.

[947] Расследование, проведенное компанией ProPublica, показало, что COMPAS дала разрозненные результаты для различных расовых групп, при этом чернокожие обвиняемые чаще подвергаются ложной маркировке высокого риска, чем белые обвиняемые, в то время как белые обвиняемые чаще подвергаются ложной маркировке низкого риска. В то время как характеристика ProPublica алгоритма как расово предвзятого была оспорена разработчиком и группой криминалистов, факт остается фактом, что чёрные ответчики с большей вероятностью несут стоимость неточностей алгоритма, чем белые ответчики. See Northpointe Inc., «COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity», (8 July 2016) <https://www.documentcloud.org/documents/2998391-ProPublica- Commentary-Final-070616.html>; Anthony Flores et al., «False Positives, False Negatives, and False Analyses: A Rejoinder to 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.'« (September 2016) 80:2 Federal Probation 38 < https:// www.uscourts.gov/sites/default/files/80_2_6_0.pdf>; Matthias Spielkamp, «Inspecting Algorithms for Bias» (12 June 2017) MIT Technology Review, <https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias>.

контексте такие модели не были развёрнуты или подтверждены.[948] Правительство Онтарио также приступило к изучению вопроса об использовании инструмента оценки рисков, аналогичного COMPAS, в решениях о предварительном заключении под стражу, и ранее оно завершило технико-экономическое обоснование таких инструментов.[949]

В контексте исправительных мер исследователи из Университета Саскачевана проводят проект машинного обучения, основанный на пересмотренной системе инвентаризации услуг уровня Онтарио (LSI-OR)[950] и предполагаемый для её замены. LSI-OR – это инструмент, который используется для проведения оценки рисков и потребностей каждые шесть месяцев для «всех взрослых заключённых, проходящих любую институциональную классификацию или решение об освобождении, для всех молодых преступников, находящихся как в безопасном, так и в открытом заключении, а также для всех условно-досрочно освобождённых.»[951]

Если эта технология будет принята, она послужит первым примером в Канаде алгоритмической технологии, используемой в контексте исправительных учреждений для непосредственного воздействия на решения о свободе личности.

В фокусе внимания № 3

Хабовая модель общественной безопасности

Модель хаба - это форма ориентированного на человека прогнозирования рисков, которая была принята рядом канадских правительственных учреждений. Этот тип программ известен под различными названиями, чаще всего «модель хаба»[952] (в Саскачеване) или «таблицы ситуаций» (в Онтарио) и описывается следующим образом:

Ситуационные таблицы предлагают место для поставщиков услуг из различных секторов (полиция, образование, наркомания, социальная работа,

---

[948] John-Etienne Myburgh, Carolyn Camman & J. Stephen Wormith, «Review of Pretrial Risk Assessment and Factors: Predicting Pretrial Release Failure» (November 2015) University of Saskatchewan, at 49<https://cfbsjs.usask.ca/documents/research/research_papers/ReviewOfPTRAandRiskFactorsPredictingPretrialReleaseFailure.pdf>.

[949] Agnese Smith, «Automating Justice» (13 March 2018) CBA National, <https://nationalmagazine.ca/en-ca/articles/law/ethics/2018/ automating-justice>.

[950] The Centre for Forensic Behavioural Science and Justice Studies, «Current Projects», University of Saskatchewan, <https://cfbsjs.usask.ca/ resea rch/current-projects. php>.

[951] Ibid.

[952] Abeba Taddese, «Saskatchewan, Canada: The Hub Model for Community Safety» Results for America, <http://results4america.org/wp- content/uploads/2017/07/LandscapeCS_Canada_4.pdf>.

психическое здоровье и т. д.) регулярно созывать и обсуждать клиентов, которые соответствуют определённому порогу риска. Цель этих дискуссий состоит в том, чтобы сформулировать план вмешательства, который мобилизует многочисленные секторы, сотрудничающие в предоставлении услуг и поддержки отдельным лицам или семьям.

Чтобы снизить риск до наступления вреда, ситуационные таблицы направлены на подключение клиентов к услугам в течение 24-48 часов с момента представления дела группе.[953]

Ситуационные таблицы предназначены для облегчения мелиоративных мер реагирования на тех, кто считается подверженным риску, а также для повышения эффективности за счёт интеграции силосов государственной службы, чтобы нуждающиеся люди не попадали в трещины между различными правительственными учреждениями. По состоянию на 2016 год в Канаде насчитывалось около 100 ситуационных таблиц. [954] Число агентств, министерств и организаций, обсуждающих и обменивающихся конфиденциальной информацией о конкретном человеке или семье, может варьироваться. Один хаб в Принс-Альберте, Саскачеван, включает по меньшей мере тринадцать,[955] в то время как «таблицы подключения» в Ватерлу, Онтарио, включают до тридцати.[956]

Такое широкое распространение модели хаба заслуживает внимания, поскольку она опирается на особую систему обмена информацией между правоохранительными органами и другими службами государственного сектора. Модель хаба не включена в качестве примера алгоритмической полицейской технологии как таковой, поскольку остается неясным, опирается ли методология, принятая в модели, на алгоритмы, когда участвующие учреждения определяют уровни риска для данного индивида или семьи. Тем не менее, потенциальное использование данных модели хаба в алгоритмических методах полицейской деятельности было признано организацией Public Safety Canada в 2015 году, когда она сообщила, что «интегрированный анализ данных здравоохранения, социальных служб, образования и уголовного правосудия поможет выявить и спланировать прогнозные модели риска на местном, региональном и провинциальном уровнях». [957] В 2019 году VICE Motherboard

---

[953] Correctional Service Canada, «Success in Reintegration: The Potential Application of Situation Tables to Community Corrections» (July 2017), <https://www.csc-scc.gc.ca/research/rr-17-02-eng.shtml> (citations omitted).
[954] Ibid.
[955]Prince Albert Community Mobilization, «CMPA Team», <https://www.srsd119.ca/departments/teacherinformation/SSS/community resources/Tri%20Fold%20Brochure%20Prince%20Albert%20Community%20Mobilization.pdf>.
[956] Carizon, Langs & Taylor Newberry Consulting, «An Evaluation of Connectivity Tables in Waterloo Region» (2017) at 1, <https://www.langs. org/about-us/publications-and-reports/connectivity-evaluation-sheet-2017.pdf>.
[957] Public Safety Canada, «Economics of Policing and Community Safety: Policy Makers' Dialogue on Privacy and Information Sharing» (January 2015) at 13 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-plcy-mdps/2015-plcy-mdps-eng.pdf>. В докладе также отмечается, что "выявление повторяющихся проблем привело к тому, что

сообщила, что конфиденциальная информация была собрана в базы данных отслеживания рисков (RTDs) в Онтарио и Саскачеване для создания индивидуальных и общинных профилей рисков.[958]

Согласно бывшему Министерству общественной безопасности и исправительных учреждений (ныне Министерство Генерального солиситора) в Онтарио, RTD «может использоваться общинами для сбора информации о местных приоритетах (т. е. рисках, уязвимых группах и защитных факторах) и развивающихся тенденциях.» [959] Министерство рекомендовало использовать эти данные «в сочетании с другими местными источниками данных из различных секторов».[960]

Алгоритмические средства наблюдения

Алгоритмические технологии используются правоохранительными органами для усиления или содействия их надзорной деятельности. Существует целый ряд алгоритмических технологий наблюдения, включая автоматизированные считыватели номерных знаков, программное обеспечение для наблюдения за социальными сетями, технологию распознавания лиц и алгоритмы анализа социальных сетей, доступные для сотрудников правоохранительных органов и в настоящее время используемые в Канаде. В этом разделе даётся обзор каждой из этих технологий и обсуждается, как они использовались или рассматриваются канадскими правоохранительными органами.

Автоматические считыватели номерных знаков

Автоматизированный считыватель номерных знаков (АСНЗ) – это «приложение для распознавания номерных знаков, в котором транспортные средства, наблюдаемые инфракрасными камерами, считывают, записывают и

провинция [Саскачеван] способствовала созданию большего числа центров ответственности (COR), с тем чтобы продолжить многосекторальную работу в направлении системных изменений и более широкого применения прогностической аналитики". Там же, в 23. В то время как предыдущий COR в Принс-Альберт, СК, был закрыт, "правительство провинции будет стремиться внедрить модель COR в Министерстве исправительных учреждений и полиции, которая будет работать со всеми 15 хабами по всей провинции". Peter Lozinski, «Centre of responsibility ceasing operations», Prince Albert Daily Herald (3 April 2019) <https://paherald.sk.ca/2019/04/03/centre-of-responsibility-ceasing-operations/>.

[958] Nathan Munn, «Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database», Vice (27 February 2019) <https://www.vice. com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>. See also Minister of Community Safety and Correctional Services, «Community Safety and Well-being Planning Framework» <https://www.mcscs.jus.gov.on.ca/english/Publications/MCSCSSSOPlanningFramework.html>.

[959] Ibid.

[960] Ibid.

проверяют свои номерные знаки в предварительно загруженной базе данных с помощью программного обеспечения для распознавания образов» [961] Камеры устанавливают на полицейских автомобилях и сканируют номерные знаки на припаркованных или движущихся транспортных средствах, когда полицейский автомобиль проезжает по общественным дорогам, или камеры устанавливаются в фиксированных положениях вдоль автомагистралей, где они сканируют номерные знаки, когда автомобилисты проезжают по шоссе. Эта технология используется правоохранительными органами в Онтарио, Британской Колумбии, Саскачеване, Альберте, Новой Шотландии, Квебеке и на острове Принца Эдуарда. Системы АСНЗ позволяют осуществлять наблюдение и профилирование путём систематического сбора объёмных данных, таких как дата, время и геолокация транспортных средств, а также регистрационной информации (т.е. идентификационной информации), связанной с этими транспортными средствами. В 2017 году уполномоченный по вопросам информации и конфиденциальности провинции Онтарио опубликовал набор необязательных руководящих принципов, в которых предлагался необходимый надзор и контроль за тем, как следует использовать этот инструмент, учитывая значительный объём информации, которая может быть получена и проанализирована с помощью этого инструмента.[962] Комиссар по вопросам информации и конфиденциальности Британской Колумбии также расследовал использование технологии АСНЗ департаментом полиции Виктории в партнёрстве с КККП и вынудил местное агентство изменить эту технологию в соответствии с законом о конфиденциальности Британской Колумбии.[963]

Наблюдение за социальными сетями

Наблюдение за социальными сетями включает в себя использование алгоритмов для сбора личной информации с платформ социальных сетей. Такая слежка предназначена для сбора информации о деятельности отдельных лиц в интернете и из неё, а также для выявления закономерностей между пользователями и связей между ними. Неалгоритмическое наблюдение за социальными сетями использовалось для мониторинга онлайн-активности вокруг таких событий, как протесты социальных движений, стремящихся к

---

[961] Robert J Howe, «Privacy Impact Assessment: Automatic License Plate Recognition (ALPR)» (October 2009) Royal Canadian Mounted Police, at 12 <https://robwipond.com/ref/RCMP%20ALPR%20PIA.pdf> (obtained through access to information request by Rob Wipond, available at https://robwipond.com/archives/831). See Christopher Parsons, «Privacy Tech-Know Blog: Who's Watching Where You're Driving?» (13 June 2017) Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/blog/20170613>.

[962] Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services [PDF].

[963] Комиссар Онтарио по вопросам информации и конфиденциальности, Руководство по использованию автоматизированных систем распознавания номерных знаков полицейскими службами (июль 2017 года) <https://www.oipc.bc.ca/investigation-reports/1480>.

равенству, и это использование вызвало озабоченность по поводу воздействия на права человека более мощных, управляемых алгоритмами версий таких инструментов. [964]

Программное обеспечение Media Sonar представляет собой яркий пример технологии наблюдения за социальными сетями. Эта компания из провинции Онтарио была запрещена на платформах Twitter и Instagram в 2016 году за нарушение политики конфиденциальности компаний социальных сетей. [965] Запрет последовал за откровением Американского союза гражданских свобод (ACLU) о том, что компания поощряла правоохранительные органы выявлять «угрозы общественной безопасности», отслеживая ключевые слова, связанные с протестом, такие как #BlackLivesMatter и связанные с ними хэштеги.[966]

По крайней мере, две канадские полицейские службы, полицейская служба Калгари (CPS) и полицейская служба Торонто (TPS), ранее использовали медиа-Сонар. Сотрудник правоохранительных органов из Калгари заявил в мае 2019 года, что, хотя Роспотребнадзор ранее использовал программное обеспечение для мониторинга «предстоящих протестов» или «чтобы почувствовать, что может произойти», он больше не использовал Media Sonar или любое другое программное обеспечение для майнинга социальных сетей, потому что компании стали менее полезными после потери доступа к основным платформам социальных сетей, таким как Facebook и Twitter.[967] У Роспотребнадзора есть письменная политика, касающаяся интернет-расследований и криминальной разведки, которая включает в себя сбор информации с сайтов социальных сетей. [968] В соответствии с этой политикой должностные лица могут собирать общедоступные данные, в том числе данные, обрабатываемые сторонними агрегаторами социальных сетей и программным обеспечением. Однако сотрудники полиции ограничиваются сбором только той

---

[964] См., например, "Используя полученную информацию [RCMP] и данные, собранные из социальных сетей, Маунти выявили 313 активистов - участников протестов по различным вопросам: от освоения природных ресурсов до пропавших без вести и убитых женщин из числа коренных народов... Затем RCMP сузил этот список до 89 человек, которые, по его словам, отвечают "критериям преступности", и создал уникальные профили для каждого из них ". Шон Крейг, "RCMP отслеживал, 89 активисты коренных народов считали" угрозами "за участие в акциях протеста", National Post (13 Ноября 2016) <https://nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests >. Правоохранительные органы, собирающие личную информацию и осуществляющие наблюдение за активистами таким образом, подвергаются серьезной критике и осуждению со стороны экспертов по правам человека и защитников гражданских свобод. Обсуждение и анализ того, как наблюдение за социальными сетями затрагивает право на приватизацию и свободу от необоснованного обыска и ареста, см. в разделе 5.2 ("Право на неприкосновенность частной жизни"). Обсуждение вопроса о слежке в социальных сетях и правах на свободу выражения мнений и свободу собраний см. в разделе 5.3 ("Права на свободу выражения мнений, мирные собрания и ассоциации").

[965] Amanda Margison, «Twitter and Instagram ban London, Ont., company for helping police track protesters» CBC News (19 January 2017) <https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093>.

[966] Matt Cagle, «This Surveillance Software is Probably Spying on #BlackLIvesMatter» (15 December 2015) ACLU NorCal, <https://www.aclunc. org/blog/surveillance-software-probably-spying-blacklivesmatter>.

[967] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

[968] Calgary Police Service, «Internet Investigations and Criminal Intelligence Ref #IN-026» (obtained through freedom of information request 18-G-1921).

информации, которая связана с конкретной целью расследования, включая «информацию, связанную с угрозой». Политика не определяет, что означает «информация, связанная с угрозой»,[969] и не ограничивает Роспотребнадзор от использования таких продуктов, как Media Sonar, в будущем, если они снова станут полезными для расследований.

TPS использовала продукт аналитики социальных сетей Sysomos,[970] базирующейся в Торонто компании, которая была приобретена компанией media intelligence Meltwater в апреле 2018 года. [971] Meltwater сделал следующее заявление о приобретении: «чтобы улучшить поиск и аналитику на платформе Sysomos, мы будем использовать модели ИИ и информацию, извлечённую из неструктурированной сети Meltwater». Meltwater также продавалась правоохранительным органам в Великобритании и США.[972] Степень, в которой TPS продолжает использовать программное обеспечение Meltwater/Sysomos или любое другое программное обеспечение для наблюдения за социальными сетями, неизвестна. (Опрошенный представитель правоохранительных органов не входил в состав соответствующего подразделения и не мог говорить по этому вопросу).[973]

В 2019 году следственные отчеты описывали расширенное использование КККП программного обеспечения для мониторинга социальных сетей, которое было предоставлено компанией Carahsoft в Соединенных Штатах. [974] Программное обеспечение под названием Social Studio было разработано компанией Salesforce для сбора и анализа массовых данных с открытым исходным кодом контента социальных сетей. RCMP использует программное обеспечение в рамках «проекта сознании». Проект Wide Awake включал в себя анализ контента социальных сетей в ходе активных расследований, а также систематическую и активную попытку предсказать преступление, которое может произойти в будущем. В ноябре 2019 года CBC News узнала из запросов FOI, что RCMP начала внутренний аудит своего мониторинга и сбора данных социальных сетей по всей Канаде, чтобы определить законность своей практики.[975]

---

[969] Ibid. at 4.
[970] R v Elliot, 2016 ONCJ 35.
[971] Mike Butcher, «Media monitor Meltwater acquires social analytics player Sysomos» (24 April 2018) Tech Crunch <https://techcrunch.com/2018/04/24/media-monitor-meltwater-acquires-social-analytics-player-sysomos/>.
[972] See North Wales Police, «2018/621 - Meltwater» (27 July 2018) <https://www.north-wales.police.uk/media/654896/2018-621-meltwater.pdf>; Brennan Center for Justice, «Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide»(16 November 2016) <https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide>.
[973] Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).
[974] Bryan Carney, «'Project Wide Awake': How the RCMP Watches You on Social Media», The Tyee (25 March 2019) <https://thetyee.ca/ News/2019/03/25/Project-Wide-Awake/>.
[975] Catharine Tunney, «RCMP launches review of its social media monitoring operation», CBC News (5 November 2019), <https://www.cbc.ca/ news/politics/rcmp-social-media-review-1.5346741>.

В апреле 2020 года RCMP опубликовала тендер на заключение контракта, в котором указывалось, что RCMP стремится расширить охват своих возможностей наблюдения за социальными сетями.[976] Согласно контрактному тендеру, одной из «обязательных» особенностей программного обеспечения, которое RCMP стремится приобрести, является то, что программное обеспечение должно быть способно выполнять следующие функции: «собирать и структурировать данные в наборы данных», которые должны храниться на серверах, расположенных в пяти странах eyes; получать доступ к источникам данных «dark web (DarkNet)»; создать базу данных с возможностью поиска, которая агрегирует «источники данных автоматически, анонимно и непрерывно» для сбора и индексирования данных.[977] RCMP указывает в своем тендере, что технология «должна обеспечивать как минимум пятнадцать источников данных, а также два источника данных Darknet или пользовательский/проприетарный алгоритм».[978] Примеры источников данных включают в себя: сайты социальных сетей (например, Facebook), микро-блогов-сайтов (таких как Twitter или Tumblr), фото- и видеосайты (такие как Instagram и YouTube), личные блоги, сайты, виртуальные миры (например, Мир Warcraft и FarmVille), «основанных на местоположении услуг» (включая «чек-инов, Facebook местах, Четвероугольного, визг»), групповые сайты покупок (такие, как Groupon), и «социальных закладок и агрегации новостей» – сайтов (таких как Digg и вкусно). [979]

В ходе неофициальных консультаций по этому докладу авторы узнали, что полиция провинции Онтарио, возможно, разработала и в настоящее время использует алгоритмическую технологию наблюдения, известную как «система онлайн-защиты детей ICAC «(ICACCOPS)»/[980]Основываясь на информации, полученной в ходе этой неофициальной консультации, представляется, что программное обеспечение ICACCOPS - это технология, которая предназначена для сканирования онлайн-чатов, использования некоторых

---

[976] Jim Bronskill, «RCMP seeks to boost social media mining for threats ranging from disease to shootings», Toronto Star (28 April 2020), <https://www.thestar.com/news/canada/2020/04/28/rcmp-seeks-to-boost-social-media-mining-for-threats-ranging-from-disease-to-shootings. html>.

[977] Public Works and Government Services Canada, «Request for a Standing Offer: Social Media Monitoring» (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF> at 12.

[978] Public Works and Government Services Canada, «Request for a Standing Offer: Social Media Monitoring» (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF> at 12.

[979] Public Works and Government Services Canada, «Request for a Standing Offer: Social Media Monitoring» (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF> at 45.

[980] United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, «ICAC Child On-line Protection System (ICACCOPS) Improvements: Award Information», <https://ojjdp.ojp.gov/funding/awards/2018-mc-fx-k063>.

автоматизированных технологических средств (неизвестного уровня сложности) для поддержания чата «открытым», чтобы сообщения автоматически не исчезали в конце разговора, а также очищать и хранить содержимое разговоров в чате в базе данных с возможностью поиска, которая доступна для правоохранительных органов. Как сообщается, эта технология, по-видимому, позволяет правоохранительным органам получать доступ к особенно частным разговорам в чате, таким как разговоры в чате с участием двух или нескольких участников в одиночку, включая чаты, защищённые паролем. Также сообщается, что по крайней мере OPP, а также региональная полицейская служба Ватерлоо (WRPS) использовали эту технологию, не запрашивая судебного одобрения в форме ордера, несмотря на то, что использование этой технологии, по-видимому, позволяет правоохранительным органам перехватывать частные сообщения. [981] Хотя существует мало общедоступной информации о базе данных ICACCOPS и нет сообщений об уголовных делах в Канаде, где использование базы данных ICACCOPS стало достоянием общественности, передняя часть программного обеспечения доступна в интернете.[982] По крайней мере в одном уголовном деле, находившемся на рассмотрении судов Онтарио (где стало известно об использовании технологии ICACCOPS OPP и WRPS), прокурор короны, как сообщается, признал, что следственный метод действительно представляет собой «gерехват» по смыслу положений Уголовного кодекса, касающихся перехвата частных сообщений, хотя корона планировала утверждать, что предварительное судебное разрешение может не потребоваться на основании

---

[981] Перехват частных сообщений - это правоохранительный метод, который требует получения предварительного судебного разрешения в виде ордера на прослушку в соответствии с Уголовным кодексом, и в Канаде перехват частных сообщений без законных полномочий является преступлением: R v TELUS Communications Co, 2013 SCC 16; R vJones, [2017] 2 SCR 696; R v Mills, 2019 SCC 22. Точное применение этих положений Уголовного кодекса, касающихся прослушивания, будет частично зависеть от возможностей технологии ICACCOPS и ее использования. Некоторые осложняющие факторы могут возникать в зависимости от географического положения правоохранительных органов, которые эксплуатируют технологию. Однако, исходя из информации, которая известна, если OPP получает постоянный доступ к технологии, которая "вмешивается в процесс связи в режиме реального времени с помощью технологических средств" (R vJones, [2017] 2 SCR 696 в пункте 72), она, вероятно, соответствовала бы определению перехвата в соответствии с Уголовным кодексом. Согласно статье 184 Уголовного кодекса перехват частных сообщений без законных полномочий является преступлением. В соответствии со статьями 193 (1), 2) (b) и 2 (e) Уголовного кодекса "использование" незаконно перехваченных частных сообщений даже для целей уголовного расследования также является преступлением согласно статье 193 Уголовного кодекса. Исключения из этого преступления предусмотрены в отношении "раскрытия" таких частных сообщений. Преступление незаконного использования перехваченных частных сообщений ранее не было предметом целенаправленного судебного анализа в Канаде, хотя соответствующая формулировка в разделе 193 в отношении "раскрытия" перехваченных частных сообщений была рассмотрена в Wakeling v Соединенные Штаты Америки, 2014 SCC 72. даже если предположить, что положения Уголовного кодекса не делают использование ICACCOPS в Канаде незаконным преступлением, тем не менее в соответствии со статьей 8 Хартии возникнут серьезные конституционные проблемы, если канадским правоохранительным органам будет разрешено обходить строгие гарантии неприкосновенности частной жизни в соответствии с положениями Уголовного кодекса, касающимися прослушивания, сознательно полагаясь на незаконно перехваченные частные сообщения, которые перехватываются иностранными правоохранительными органами и становятся доступными в Канаде в режиме реального времени.

[982] <https://www.icaccops.com/users/login.aspx?ReturnUrl=%2Fusers> (accessed 30 April 2020).

теории о том, что это материал с открытым исходным кодом. [983]Дело было прекращено короной позднее, поэтому не привело к дальнейшим судебным разбирательствам или каким-либо судебным решениям по этому вопросу закона.

В то время как OPP разрабатывала этот инструмент, авторы получили информацию о том, что OPP установила контакт со своими американскими коллегами по поводу этого инструмента, и база данных ICACCOPS в настоящее время эксплуатируется и поддерживается в Соединённых Штатах для использования правоохранительными органами, причём доступ к ней предоставляется следователям, например, в OPP и WRPS. OPP и WRPS станут первыми канадскими правоохранительным органами, публично сообщившими об использовании этой технологии. В документе 2018 года, касающемся финансирования дальнейших исследований по расширению возможностей наблюдения, Министерство юстиции Соединённых Штатов неявно предположило, что технология ICACCOPS является одной из потенциально многочисленных технологий, которые были разработаны для «эффективного и действенного анализа цифровых доказательств, ускорения сбора доказательств и передачи цифровых файлов, облегчения дешифровки, решения проблем шифрования мобильных чатов, автоматизации разведки данных», и поддерживать [программу целевой группы по интернет-преступлениям против детей (ICAC)].[984] В частности, в одной заявке на финансирование, поданной в Министерство Юстиции, говорилось, что «ICACCOPS поддерживает расследования интернет-чатов, онлайн-вымогательств, соблазнов и тёмной веб-активности.» [985]Авторы этого отчёта не получали никакой информации через запросы FOI, которые раскрывали бы, что OPP может использовать эту технологию.

Центр стратегических операций полицейской службы Оттавы (OPSOC), как сообщается, также развернул форму наблюдения за социальными сетями. Согласно статье VICE Motherboard, OPSOC предоставляет «виртуальное резервное копирование» патрульным подразделениям полицейской службы Оттавы, выполняя анализ информации, полученной из полицейских баз данных и онлайн-источников, в режиме реального времени. Эти анализы призваны обеспечить офицерам ситуационную осведомленность о данной сцене. На

---

[983]По-видимому, позиция Короны не является правильной в том, что разговоры в чате действительно являются материалами с "открытым исходным кодом", учитывая, что инструмент, по-видимому, соскребает даже защищенные паролем разговоры, включая разговоры в чатах, в которых может быть всего два человека: see R v Mills, 2019 SCC 22 at para 24; R v Marakah, 2017 SCC 59 at paras 28 and 55.

[984] United States Department of Justice, «OJJDP FY 2018 Strengthening Investigative Tools and Technology for Combating Child Sexual Exploitation», OMB No 1121-0329, <https://ojjdp.ojp.gov/sites/g/files/xyckuh176/files/media/document/OJJDP-2018-14460.PDF> at 5.

[985] United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, «ICAC Child On-line Protection System (ICACCOPS) Improvements: Award Information», <https://ojjdp.ojp.gov/funding/awards/2018-mc-fx-k063>.

момент написания статьи публично неизвестно, имеет ли OPSOC в настоящее время какую-либо форму алгоритмической или прогностической аналитики или использует её. Однако сообщается, что OPSOC разрабатывает алгоритмические возможности в дополнение к своим нынешним возможностям. [986]

4.3.3. Распознавание лиц

Программное обеспечение для распознавания лиц - это технология биометрической идентификации, которая использует «компьютерные алгоритмы для выделения конкретных, отличительных деталей о лице человека из фотографии, серии фотографий или видеосегмента. Эти детали, такие как расстояние между глазами или форма подбородка, затем преобразуются в математическое представление и сравниваются с данными о других лицах, ранее собранными и сохранёнными в базе данных распознавания лиц» [987]Распознавание лиц может принимать форму «один к одному», которая сравнивает лицо с фотографией конкретного человека в базе данных, чтобы убедиться, что человек является тем, за кого он себя выдает, или «один ко многим», которая сравнивает лицо со всеми фотографиями в базе данных, чтобы определить, кто этот человек. [988]

Фотографии, сделанные с помощью кружек, собираются в соответствии с законом об идентификации преступников, который предусматривает, что лица могут быть сфотографированы без их согласия, если они обвиняются, осуждены или предположительно совершили преступление, подлежащее обвинению. [989]Как полицейская служба Калгари (CPS), так и полицейская служба Торонто (TPS) используют программное обеспечение для распознавания лиц от корпорации NEC-подтверждённое как NeoFace Reveal в случае CPS[990] - для поиска фотографий и составных рисунков неизвестных лиц в базах данных агентств по фотографиям. Роспотребнадзор также сохраняет неопознанные изображения, чтобы искать их по новым фотографиям, которые

---

[986] Nathan Munn, «'Predictive Policing' Is Coming to Canada's Capital, and Privacy Advocates Are Worried», VICE Motherboard (13 February 2017) <https://www.vice.com/en_us/article/jpaew3/ottawa-police-strategic-operations-centre-canada-surveillance>.

[987] Jennifer Lynch, «Face Off: Law Enforcement Use of Face Recognition Technology» (February 2018) Electronic Frontier Foundation, at 4-5, <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf>.

[988] Future of Privacy Forum, «Understanding Facial Detection, Characterization and Recognition Technologies» (March 2018) <https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf>.

[989] Calgary Police Service, «Facial Recognition Technology, Ref #IN-006-1» at 1 (obtained through freedom of information request 18-G-1921); Identification of Criminals Act, RSC 1985, c I-1, s. 2(1); Identification of Criminals Act, RSC 1985, c I-1, s. 2(1).

[990] «Facial Recognition To Aid Investigations», City of Calgary Newsroom (3 November 2014) <https://newsroom.calgary.ca/facial-recognition- to-aid-investigations/>; Kate Allen and Wendy Gillis, «Toronto police have been using facial recognition technology for more than a year», Toronto Star (28 May 2019) <https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html>.

впоследствии собираются.[991] Полицейская служба Оттавы (OPS) провела трёхмесячную пилотную программу с NeoFace Reveal, закончившуюся в марте 2019 года, и заявила, что в настоящее время они не используют этот продукт.[992] Полицейская служба Эдмонтона (EPS) также недавно объявила, что планирует использовать технологию распознавания лиц в отношении своей базы данных mug-shot к концу 2020 года. [993]Аналогичным образом, в 2020 году стало известно, что региональная полиция Йорка выделила в 2019 году 1,68 миллиона долларов на приобретение системы распознавания лиц и автоматизированной системы распознавания ладоней и отпечатков пальцев в какой-то момент между 2019 и 2021 годами. [994] В региональной полицейской службе пила подтвердили, что они также получат лицензию на использование той же системы. Как CPS, так и TOS утверждают, что совпадения по распознаванию лиц не предназначены для использования в качестве бесспорной положительной идентификации и, вместо этого, предназначены только для обеспечения следственных зацепок. [995]Предварительное судебное разрешение не может быть получено до того, как специализированный персонал CPS или TPS проведет запрос распознавания лиц с помощью этого программного обеспечения. [996]В 2012 году уполномоченный по вопросам информации и конфиденциальности Британской Колумбии установил, что VPD использовала технологию распознавания лиц и фотографии водительских прав, которые хранились государственным автомобильным страховщиком провинции, без получения индивидуального согласия или предварительного судебного разрешения. [997]Комиссар приказал прекратить эту практику без ордера.

По состоянию на февраль 2020 года федеральные и провинциальные регуляторы конфиденциальности расследовали использование компании по распознаванию лиц Clearview AI после сообщения о том, что компания продавала свои услуги более чем 600 правоохранительным органам, главным

---

[991] Calgary Police Service, «Facial Recognition 2018» at 10 (obtained through freedom of information request 18-G-1921).

[992] Shaamini Yogaretname, «Ottawa police piloted controversial facial recognition software last year», Ottawa Citizen (14 February 2020) <https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-last-year/>; and Shaamini Yogaretnam, «Chief says facial recognition software test drew on police mug shot database», Ottawa Citizen (26 February 2020) <https:// ottawacitizen.com/news/local-news/chief-says-facial-recognition-software-test-drew-on-police-mug-shot-database/>.

[993] Anna Junker, «Edmonton police unveil details on use of facial recognition technology», The Edmonton Journal (19 February 2020), <https://edmontonjournal.com/news/local-news/edmonton-police-unveil-details-on-use-of-facial-recognition-technology>.

[994] Nathan Munn, «Police Forces in Canada Are Quietly Adopting Facial Recognition Tech», VICE Media (23 June 2020), <https://www.vice.com/ en_ca/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech>.

[995] Mark Saunders, «Toronto Police Services Board Report: Facial Recognition System» (17 May 2019) at 2 <http://www.tpsb.ca/images/ agendas/PUBLIC_AGENDA_May30.pdf>.

[996] Ibid. at 3.

[997] Office of the Information & Privacy Commissioner, «Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia» (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

образом в Соединенных Штатах. [998] Clearview AI, как сообщается, собрал около 3 миллиардов изображений из интернета и объединил их для использования в расследованиях правоохранительных органов. Продолжающиеся репортажи средств массовой информации в Канаде привели к открытию того, что КККП, сотрудники полицейской службы Калгари и Эдмонтона, [999] а также многочисленные полицейские службы по всему Онтарио, включая TPS, региональную полицейскую службу, полицейскую службу Холтона, полицейскую службу Оттавы, региональную полицейскую службу Дарема, региональную полицейскую службу Ниагары и полицейскую службу Гамильтона, использовали ИИ Clearview.[1000] Эти разоблачения произошли только после того, как некоторые агентства отрицали использование этого инструмента, предположительно из-за того, что не осознавали, что отдельные сотрудники занимались несанкционированным использованием ИИ Clearview в своей работе.[1001] Кроме того, FOI records указала, что КККП «отрицала использование программного обеспечения для распознавания лиц на канадцах через три месяца после того, как она заключила контракт со спорной американской компанией Clearview AI», согласно сообщению Tyee.[1002] Хотя Clearview AI объявила в июле 2020 года, что больше не будет предлагать услуги распознавания лиц в Канаде, и на неопределённый срок приостановила свой контракт с КККП, [1003] это всего лишь одна из многих компаний, предлагающих такие услуги. Технология распознавания лиц как категория остаётся постоянной проблемой в Канаде.

---

[998] Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It», The New York Times (18 January 2020), <https://www. nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; «Privacy watchdogs to probe Clearview AI's facial-recognition technology», CBC News (21 February 2020), <https://www.cbc.ca/news/canada/toronto/clearview-ai-police-use-1.5471493>.

[999] «Как полицейская служба Калгари, так и полицейская служба Эдмонтона в начале этого месяца отрицали использование программного обеспечения, но с тех пор оба получили сообщения о том, что несколько их сотрудников протестировали программное обеспечение Clearview AI. Старший сержант Гордон Макдональд из секции уголовной идентификации полиции Калгари сказал, что служба не будет интересоваться программным обеспечением, которое использует изображения с открытым исходным кодом из-за этических соображений ". Alanna Smith, «Two Calgary officers tested Clearview AI facial-recognition software», Calgary Herald (29 February 2020). <https://calgaryherald. com/news/loca l-news/two-calgary-officers-tested-clea rview-a i-facial-recognition-software/>.

[1000] «Toronto police admit using secretive facial recognition technology Clearview AI», CBC News (13 February 2020) <https://www.cbc.ca/ news/canada/toronto/toronto-police-clearview-ai-1.5462785>; Kelly Bennett, «Hamilton police tested controversial facial recognition technology Clearview AI», CBC News (20 February 2020), <https://www.cbc.ca/news/canada/hamilton/the-service-says-it-has-not-used-the-tool-for-any- investigative-purposes-1.5470359>; Shaamini Yogaretnam, «Ottawa police piloted controversial facial recognition software last year», Ottawa Citizen (13 February 2020), <https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-last- year>.

[1001] Смотрите, например, "Полиция Торонто признает использование технологии скрытного распознавания лиц Clearview AI", CBC News (13 February 2020) <https://www. cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785>.

[1002] Bryan Carney, «FOI Documents Confirm RCMP Falsely Denied Using Facial Recognition Software», The Tyee (16 April 2020) <https://thetyee. ca/News/2020/04/16/RCMP-FOI-Facial-Recognition/>.

[1003] Office of the Privacy Commissioner of Canada, «Clearview AI ceases offering its facial recognition technology in Canada» (6 July 2010) <https://priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/>.

Технология распознавания лиц также была предметом широкого беспокойства и всё более решительных действий в Соединенных Штатах. На момент написания статьи четыре города запретили использование технологии распознавания лиц правительством и правоохранительными органами: Бостон и Сомервилл в штате Массачусетс, [1004]а также Сан-Франциско и Окленд в штате Калифорния.[1005] Кроме того, в июне 2020 года Ассоциация вычислительной техники (ACM) США Technology Policing Committee (USPTC) публично призвала «немедленно приостановить текущее и будущее частное и правительственное использование технологий распознавания лиц (FR) во всех известных или разумно предсказуемых обстоятельствах, которые могут нанести ущерб установленным правам человека и законным правам». [1006]В своём заявлении о принципах ACM USPTC представила свои выводы о том, что технология распознавания лиц «недостаточно зрела и надёжна для безопасного и справедливого использования без надлежащих гарантий против неблагоприятного воздействия на отдельных лиц, особенно на уязвимые группы населения» и что «её использование часто ставит под угрозу основные права человека и юридические права отдельных лиц на неприкосновенность частной жизни, занятость, правосудие и личную свободу». [1007]

Крупные технологические игроки добавили свой вес к озабоченности по поводу распознавания лиц, способствуя растущей волне вопросов о ценности и влиянии этой технологии. IBM публично отказалась от дальнейшей разработки или продажи технологии распознавания лиц, сославшись на озабоченность расовым профилированием со стороны полиции. [1008]

Microsoft заявила, что она откажется продавать свою технологию распознавания лиц полицейским службам до тех пор, пока не будут приняты

[1004] Sean Philip Couter, «Boston City Council votes to ban facial-recognition technology», Boston Herald (24 June 2020) <https://www. bostonherald.com/2020/06/24/boston-city-council-votes-to-ban-facial-recognition-technology/>; and Caroline Haskins, «A Second U.S. City Has Banned Facial Recognition», VICE Motherboard (28 June 2019) <https://www.vice.com/en_ca/article/paj4ek/somerville-becomes-the-second-us- city-to-ban-facial-recognition>.

[1005] Kate Conger, Ricahrd Fausset & Serge F Kovaleski, «San Francisco Bans Facial Recognition Technology,» New York Times (14 May 2019) <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>; and Sarah Ravani, «Oakland bans use of facial recognition technology, citing bias concerns,» San Francisco Chronicle (17 July 2019) <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of- facial-recognition-14101253.php>.

[1006] ACM является "крупнейшим в мире образовательным и научным вычислительным обществом", а его USTPC "служит центром взаимодействия ACM со всеми ветвями правительства США, вычислительным сообществом и общественностью по вопросам политики, связанным с информационными технологиями". «ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies» (30 June 2020), Association for Computing Machinery <https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition- technologies>.

[1007] Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies» (30 June 2020), ACM US Technology Policy Committee <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech- statement.pdf>.

[1008] Alex Hern, «IBM quits facial-recognition market over police racial-profiling concerns,» Guardian (9 June 2020) <https://www.theguardian. com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns>; and Jay Peters, «IBM will no longer offer, develop, or research facial recognition technology,» The Verge (8 June 2020) <https://www.theverge.com/2020/6Z8/21284683/ibm-no-longer- general-purpose-facial-recognition-analysis-software>.

федеральные законы, регулирующие её использование. [1009]Amazon наложила на себя однолетний мораторий на продажу технологии распознавания лиц полицейским службам, якобы для того, чтобы «дать Конгрессу достаточно времени» для выполнения правил.[1010]Google также заявила о поддержке временного запрета на технологию распознавания лиц.[1011]

В 2019 году компания Axon Enterprise (ранее TASER) запретила использовать системы распознавания лиц в своих камерах наблюдения за телом.[1012] Хотя эти отраслевые позиции подвергались критике за недостаточность, своекорыстие, оппортунизм или неэффективность, [1013] тот факт, что даже доминирующие поставщики технологии распознавания лиц сочли нужным взять на себя такие обязательства в какой-либо степени, является еще одним свидетельством высокого риска этой технологии в отношении ее воздействия на конституционные права и свободы человека.[1014]

[1009] Jay Greene, «Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM,» Washington Post (11 June 2020) <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/>.

[1010] «We are implementing a one-year moratorium on police use of Rekognition» (10 June 2020), Amazon <https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>; Karen Weise & Natasha Singer, «Amazon Pauses Police Use of Its Facial Recognition Software,» New York Times (10 June 2020) <https://www.nytimes.com/2020/06/10/technology/amazon-facial- recognition-backlash.html>.

[1011] Michael Kan, «Google: Temporary Ban on Facial-Recognition Tech Might Be Necessary,» PCMag (21 January 2020) <https://www.pcmag. com/news/google-temporary-ban-on-facial-recognition-tech-might-be-necessary>.

[1012] Charlie Warzel, «A Major Police Body Cam Company Just Banned Facial Recognition,» New York Times (27 June 2019) <https://www.nytimes. com/2019/06/27/opinion/police-cam-facial-recognition.html>.

[1013] See e.g., Zack Whittaker, «Amazon's facial recognition moratorium has major loopholes,» Techcrunch (10 June 2020) <https://techcrunch. com/2020/06/10/amazon-rekognition-moratorium/>; Will Knight, «IBM's Withdrawal Won't Mean the End of Facial Recognition,» Wired (10 June 2020) <https://www.wired.com/story/ibm-withdrawal-wont-mean-end-facial-recognition/>; Kate Kaye, «IBM, Microsoft, and Amazon's face recognition bans don't go far enough,» Fast Company (13 June 2020) <https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons- face-recognition-bans-dont-go-far-enough>; Laurie Clarke, «Amazon's facial recognition stunt is pure PR,» New Statesman Tech (10 June 2020) <https://tech.newstatesman.com/security/amazons-facial-recognition-stunt>; «Why Amazon's temporary ban of police use of facial recognition is not enough» (11 June 2020), Privacy International, <https://privacyinternational.org/news-analysis/3896/why-amazons-temporary-ban-police- use-facial-recognition-not-enough>.

[1014] Подробный анализ технологии распознавания лиц и ее высокого риска нарушения и ухудшения права на неприкосновенность частной жизни см. в разделе 5.2.4 "IN FOCUS # 5: Facial Recognition Technology and the Erosion of Privacy Rights" ("Точность данных: неточные данные и неточные алгоритмы") настоящего отчета.

Анализ социальных сетей

Анализ социальных сетей (ACC) «основан на предпосылке, что отношения между индивидами могут информировать и даже предсказывать поведение индивида.[1015] ACC «использует статистические методы и методы визуализации для описания того, как социальные субъекты подвергаются воздействию окружающих их людей и, в свою очередь, как эти индивиды влияют на акторов, с которыми они связаны, и как набор акторов и отношения между ними влияют на поведение в реальном мире»,например, преступную деятельность. [1016]Доступность машинного обучения в сочетании с ростом слежки за социальными сетями, распознаванием номерных знаков, технологиями распознавания лиц и другими инструментами массового наблюдения для сбора информации побудили различные правоохранительные органы сосредоточить своё внимание на потенциальном использовании ACC в контексте алгоритмической полицейской деятельности.[1017]

В дополнение к полицейской службе Калгари, участвующей в ACC, как описано выше в разделе 4.2.1 («полицейская служба Калгари: Palantir и IBM i2 Analyst Notebook»), в документе, подготовленном по заказу Министерства общественной безопасности Канады в 2012 году, был разработан и предложен инструмент ACC. Этот инструмент автоматически выявлял бы преступные организации в больших наборах данных социальных сетей и основывался бы на сетевом анализе данных полиции Британской Колумбии о соучастниках преступлений.[1018] Кроме того, в своей политике по искоренению расового профилирования в правоохранительных органах комиссия по правам человека Онтарио определила анализ социальных сетей как потенциальный источник неблагоприятного воздействия на расовые сообщества, где задействована алгоритмическая полицейская деятельность.[1019]

[1015] Andrew Papachristos & Michael Sierra-Arevalo, «Policing the Connected World» (2018) Office of Community Oriented Policing Services, at viii <https://ric-zai-inc.com/Publications/cops-w0859-pub.pdf>.
[1016] Ibid.
[1017] See e.g., Andrew Papachristos & Michael Sierra-Arevalo, «Policing the Connected World» (2018) Office of Community Oriented Policing Services, at 21 <https://ric-zai-inc.com/Publications/cops-w0859-pub.pdf>.
[1018] Uwe Glasser et al., «Estimating Possible Criminal Organizations from Co-offending Data» (November 2012) Public Safety Canada, <http:// publications.gc.ca/collections/collection_2012/sp-ps/PS14-7-2012-eng.pdf>; see also Public Safety Canada, «Organized Crime Research Brief no. 28: Data mining for Possible OC» at 1-2 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rgnzd-crm-brf-28/index-en.aspx>.
[1019] Ontario Human Rights Commission, «Policy on eliminating racial profiling in law enforcement» at 4.2.6.2, <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

Ограничения результатов исследований

Выводы, приведённые в части 4, описывают, как правоохранительные органы по всей Канаде начали рассматривать, разрабатывать или использовать различные алгоритмические методы полицейской деятельности. Однако этот обзор не обязательно представляет собой полный фактический отчёт о том, в какой степени правоохранительные органы Канады используют или разрабатывают алгоритмические полицейские технологии. Это объясняется, по меньшей мере, тремя причинами: отсутствием прозрачности со стороны правоохранительных органов в отношении использования ими новых технологий полицейского надзора, барьерами для доступа к информации в рамках канадских процессов запроса FOI и способностью правоохранительных органов претендовать на привилегии в отношении информации, которая в противном случае была бы раскрыта в ответ на запрос FOI. В оставшейся части этого раздела мы обсудим каждое из этих ограничений исследования.

Во-первых, правоохранительные органы исторически воздерживались от раскрытия информации об использовании ими новых технологий полицейского надзора.[1020] Уклонение от раскрытия информации об использовании новой технологии наблюдения включает, например, снятие уголовных обвинений, по-видимому, для того, чтобы избежать необходимости раскрывать детали использования симуляторов сотовых сайтов (также известных как IMSI catchers), которые имитируют вышки сотовой связи для захвата личных данных с мобильных телефонов людей. [1021] К сожалению, для канадской общественности нет ничего необычного в том, что она узнаёт об использовании или развитии новых полицейских технологий только после того, как они были использованы или испытаны полицейскими ведомствами в течение длительного периода времени. Прозрачность является важным компонентом существующих в Канаде механизмов полицейского надзора и подотчётности, без которых законодатели не могут давать руководящие указания правоохранительным органам или надлежащим образом регулировать их деятельность. Прозрачность также позволяет директивным органам и

[1020] Например, в 2017 году общественность узнала, что RCMP реализовал спорную программу анализа метаданных только после того, как от программы позже отказалось агентство: Jim Bronskill, «RCMP created metadata-crunching tool to glean criminal intelligence», Global News (9 May 2017), <https://globalnews.ca/news/3437034/rcmp-created-metadata-crunching-tool-to-glean-criminal-intelligence/>. See also, Kate Allen & Wendy Gillis, «Toronto police have been using facial recognition technology for more than a year», Toronto Star (28 May 2019), <https://www. thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html>.

[1021] Justin Ling, «A mob trial is over after Canadian cops refuse to disclose their surveillance techniques», Vice (21 March 2017), <https://www. vice.com/en_ca/article/ywn7gm/a-mob-trial-is-over-after-canadian-cops-refuse-to-disclose-their-surveillance-techniques>. See generally Tamir Israel & Christopher Parsons, «Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada» (August 2016), Citizen Lab <https:// citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>.

общественности более эффективно рассматривать и разрабатывать обоснованные законы и политику в отношении диапазона ограничений, которые необходимы для защиты конституционных прав и прав человека и обеспечения баланса государственных интересов.[1022]Тем не менее, несмотря на некоторые принятые меры по обеспечению прозрачности, по-прежнему остаётся нереалистичным предполагать, что общественность Канады в настоящее время имеет доступ к полной фактической информации о том, в какой степени в настоящее время используются технологии алгоритмической полицейской деятельности.

Во-вторых, существует множество проблем, связанных с процессами запроса FOI в Канаде.

К числу таких проблем относятся, например, значительные задержки, сложность разработки достаточно широких или точно определённых условий запроса, высокие сборы за обработку и большое число правоохранительных учреждений и связанных с ними учреждений на муниципальном, провинциальном и федеральном уровнях. Таким образом, невозможно сделать вывод о том, что документы, на которые опирался автор настоящего доклада, являются исчерпывающим описанием алгоритмических полицейских технологий, используемых или разрабатываемых канадскими правоохранительными органами.

В качестве одного из примеров неадекватности процесса запроса FOI в мае 2019 года общественности стало известно, что TPS приобрела систему распознавания лиц в марте 2018 года и не раскрыла её общественности. [1023]Авторы этого доклада ранее направили запрос FOI в TPS, который включал широкий запрос на записи, касающиеся распознавания лиц, в течение периода времени, включающего март 2018 года. TPS не предоставила никакой информации или отзывчивых документов относительно использования распознавания лиц, несмотря на то, что теперь известно, что полицейская служба потратила 451 718 долларов на систему распознавания лиц в течение периода времени, который был предметом запроса FOI. [1024] Несколько запросов FOI от различных агентств остаются невыполненными даже на момент написания настоящего доклада.

[1022] Транспарентность уже была определена в качестве одного из основных принципов Директивы правительства Канады об автоматизированном принятии решений, в которой прозрачность определяется как один из основных принципов, определяющих интеграцию искусственного интеллекта и автоматизированного принятия решений в сфере услуг государственного сектора: Government of Canada, «Directive on Automated Decision-Making» (5 February 2019) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

[1023] Kate Allen and Wendy Gillis, «Toronto police have been using facial recognition technology for more than a year", Toronto Star (28 May 2019) <https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html>.

[1024] Phillip Lee-Shanok, «Privacy advocates sound warning on Toronto police use of facial recognition technology", CBC News (30 May 2019), <https://www.cbc.ca/news/canada/toronto/privacy-civil-rights-concern-about-toronto-police-use-of-facial-recognition-1.5156581>.

В-третьих, во многих случаях запросы FOI были возвращены с ответами, которые требовали привилегии, то есть утверждения о том, что отвечающее агентство не раскрывает и не обязано раскрывать запрашиваемые материалы по юридическим причинам. Основываясь на этих ответах, некоторые правоохранительные органы могут утверждать привилегии в отношении некоторых алгоритмических методов полицейской деятельности, которые разрабатываются или используются, если агентство занимает позицию, что такие методы подлежат привилегиям расследования. Следственная привилегия используется правительственными учреждениями и, если это законно, позволяет правоохранительным органам сохранять конфиденциальность определённых полицейских методов, которые в противном случае были бы раскрыты в рамках данного юридического процесса (например, через запрос FOI). Такая привилегия должна устанавливаться правоохранительным органом в каждом конкретном случае. Для обоснования обоснованности притязания на следственную привилегию соответствующая информация должна: 1) использоваться полицейским учреждением в качестве правоохранительного органа, 2) не быть публично известной и 3) быть способной помочь потенциальным правонарушителям вмешаться в следственные функции полиции или помешать им в случае её разглашения.[1025] Из-за нехватки времени авторы не обжаловали эти претензии специально уполномоченным по вопросам информации и конфиденциальности для вынесения решения о целесообразности использования правоохранительными органами следственных привилегий; таким образом, ещё предстоит выяснить, являются ли их претензии на привилегии в отношении алгоритмических полицейских технологий обоснованными или нет.[1026]

4.5. Заключительные замечания: современное состояние алгоритмической полиции в Канаде

Таким образом, выводы, содержащиеся в части 4, демонстрируют, что алгоритмические технологии используются и находятся в стадии разработки или рассматриваются в различных контекстах, связанных с полицейской деятельностью в Канаде. По меньшей мере две полицейские службы, департамент полиции Ванкувера и полицейская служба Саскатуна, разработали или разрабатывают алгоритмические полицейские технологии для целей руководства действиями и вмешательством полиции. Другие полицейские

[1025] R vAmer, 2017 ABQB 651 at para 37

[1026] See Tamir Israel & Christopher Parsons, Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada (August 2016) at 31¬49, <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>, discussing the meaningful limits of investigative privilege in greater detail in a similar context relating to another novel policing technology.

службы, например, в Калгари и Торонто приобрели технологические инструменты, которые используются юрисдикциями за пределами Канады для создания алгоритмических полицейских систем. Кроме того, многие правоохранительные органы используют алгоритмические технологии наблюдения (например, автоматизированные считыватели номерных знаков, алгоритмы распознавания лиц и мониторинга социальных сетей) или разрабатывают такие технологии.

В то же время, судя по официальным исследовательским интервью и кабинетным исследованиям, проведённым для настоящего доклада, использование алгоритмических полицейских систем, по-видимому, не получило широкого распространения в Канаде, даже если фактические данные по этому вопросу не являются окончательными. Относительно низкий уровень внедрения этих технологий канадскими полицейскими службами может быть результатом ряда потенциальных факторов, включая осторожные подходы директивных органов и правоохранительных органов к внедрению или интеграции алгоритмических технологий, а также бюджетные или ресурсные ограничения, которые ограничивают закупку или использование этих технологий.

Именно на фоне результатов исследований, представленных в разделах 4.1-4.4, в части 5 («Международные последствия алгоритмической полицейской деятельности в области прав человека и прав Хартии») излагается правовой и политический анализ последствий алгоритмической полицейской деятельности для прав человека и конституционного права. Несмотря на кажущееся (на момент написания статьи) относительное отсутствие широкого развития или внедрения этих технологий в Канаде, из представленных выше результатов исследований очевидно, что алгоритмические полицейские технологии используются, находятся в стадии разработки или рассматриваются в различных контекстах, связанных с правоохранительной деятельностью в Канаде. Таким образом, анализ этих технологий через призму прав человека и конституционного права не только оправдан, но и назрел. Именно посредством оценки последствий применения этого класса правоохранительных технологий для прав человека и конституционного права общество может обеспечить, чтобы их использование или потенциальное развитие не приводило к несправедливому нарушению основных прав и свобод человека и общества, подвергшихся воздействию.

Международные права человека и хартия прав - последствия алгоритмической полицейской деятельности

Алгоритмические полицейские технологии поднимают целый ряд правовых и политических вопросов, которые затрагивают несколько прав человека, защищаемых в канадской хартии прав и свобод («Хартия»)[1027] и в международном праве прав человека. В части 5 настоящего доклада представлены и проанализированы последствия использования технологии алгоритмической полицейской деятельности через призму некоторых из этих прав. Канадское и международное право прав человека гарантируют права человека, рассматриваемые в настоящем докладе; соответственно, каждое право анализируется в рамках обоих правовых режимов.

В разделе 5.1 даётся общий обзор внутреннего и международного законодательства, регулирующего обязательства Канады в области прав человека, и излагается подход авторов к анализу алгоритмических полицейских технологий в области прав человека. В последующих разделах части 5 каждый из них анализирует алгоритмическую полицейскую деятельность через призму конкретного права человека: право на неприкосновенность частной жизни (раздел 5.2); право на свободу выражения мнений, мирных собраний и ассоциаций (раздел 5.3); право на равенство и свободу от дискриминации (раздел 5.4); право на свободу и свободу от произвольного задержания (раздел 5.5); право на надлежащую правовую процедуру (раздел 5.6); и право на правовую защиту (раздел 5.7). В каждом разделе кратко излагается рассматриваемое право и то, как оно защищается в канадском и международном праве, а затем анализируются конкретные вопросы и проблемы, возникающие в связи с этим правом в рамках алгоритмической полицейской технологии.

Введение в анализ алгоритмической полицейской деятельности в области прав человека

Обязательства Канады в области прав человека регулируются уставом, квазиконституционным внутренним законодательством и международными договорами по правам человека, которые она ратифицировала. Все действия правительства должны соответствовать этим законам, включая действия, связанные с алгоритмическими полицейскими методами, которыми занимаются правоохранительные органы. Правовой анализ, представленный в настоящем докладе, прямо опирается на международные права человека в качестве дополнительного источника обязательств Канады в области прав человека по двум причинам.

[1027] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Во-первых, международное право прав человека может обеспечить международную нормативную моральную силу, которая обязывает правительства и предприятия соблюдать определённые всеобъемлющие стандарты и обязательства в области прав человека. Международное право в области прав человека выступает в качестве внешнего стандарта, устанавливая систему отсчёта, в соответствии с которой оцениваются действия канадского государства (in). Это особенно важно, когда правительства должны рассмотреть вопрос о том, как использовать новые технологии или технологии, которые ещё не подверглись независимой юридической проверке. Такие технологии часто могут поднимать новые вопросы, которые ещё не были предметом Конституционного судебного разбирательства в Канаде.

Во-вторых, международные обязательства в области прав человека являются составной частью правовой системы Канады. Канада обязана соблюдать и выполнять свои международные обязательства в области прав человека в рамках международной правовой системы. В рамках национальной правовой системы запретительные нормы международного обычного права автоматически инкорпорируются во внутреннее право, а международные договоры или Конвенции приобретают обязательную силу в канадском праве, если они вступают в силу в рамках внутреннего законотворческого процесса Канады. [1028] Конечно, верно, что Канада как суверенное государство может отменять международные договоры и обычное право посредством внутреннего законодательства, противоречащего этим обязательствам.[1029] Тем не менее внутреннее законодательство должно соответствовать Конституции Канады. При применении Хартии её текст часто будет толковаться как обеспечивающий защиту по меньшей мере в той же степени, в какой она обеспечивается аналогичными положениями международных документов по правам человека, участником которых является Канада. [1030]

В результате, если полицейская практика, связанная с использованием алгоритмических полицейских технологий, нарушает международные обязательства в области прав человека, канадское правительство несёт ответственность за принятие законодательных или других соответствующих мер для приведения такой полицейской практики в соответствие с этими обязательствами. Кроме того, все внутреннее законодательство должно соответствовать уставу, толкование которого основывается на международных обязательствах в области прав человека.

[1028] R v Hape, [2007] 2 SCR 292 at para 39; Kazemi Estate v Islamic Republic of Iran, 2014 SCC 62 at para 149.
[1029] Ibid.
[1030] Kazemi Estate v Islamic Republic of Iran, 2014 SCC 62 at para 150.

Общественная информация о том, в какой степени в Канаде используются алгоритмические полицейские технологии, является неполной.[1031] В результате правовой и политический анализ в разделах 5.2-5.7 обязательно носит перспективный характер. В некоторых случаях анализ носит гипотетический характер, поскольку он основан на соответствующей литературе, прецедентах и исследованиях алгоритмических полицейских технологий в других юрисдикциях, в частности в Соединённых Штатах и Соединённом Королевстве. Некоторые проблемы - такие как проблема чёрного ящика, петли обратной связи и уклон автоматизации - появляются несколько раз на протяжении всего анализа прав человека из-за их сквозного характера и потому, что они затрагивают несколько прав одновременно.

Учитывая стремительное развитие технологий и их тенденцию опережать правовые гарантии прав человека, анализ настоящего доклада служит руководством к потенциальным проблемам в области прав человека, которые должны быть приняты во внимание, если канадские полицейские службы продолжат или расширят использование алгоритмических полицейских технологий. В отсутствие осторожности и должной осмотрительности существует серьёзный риск того, что права человека и права, закреплённые в Уставе, станут второстепенными в соответствующих законах, политике и дискуссиях, а не необходимой отправной точкой.

В фокусе внимания № 4

Бизнес и права человека

В настоящем докладе основное внимание уделяется конституционным и правозащитным обязательствам канадского правительства и канадских правоохранительных органов, но частный сектор также играет определённую роль в разработке и внедрении правоохранительных технологий, в том числе в области алгоритмической полицейской деятельности. Многие из стратегий полицейской деятельности, рассмотреные в настоящем докладе, требуют технической и технической помощи со стороны частных компаний. В некоторых случаях полицейские службы приобретают готовые решения, такие как Prepol, который разрабатывается и полностью принадлежит частной компании. В других случаях правоохранительные органы могут сотрудничать с

[1031] Объяснение того, почему информация является неполной, связано с проблемами, изложенными в разделе 1.2 ("Методология") и разделе 4.4 ("Ограничения результатов исследований"). Он включает в себя утверждения о привилегиях, невыполненные просьбы ФОИ, отсутствие транспарентности среди некоторых полицейских служб и отсутствие общедоступной информации об использовании обследованных технологий канадскими полицейскими службами.

частными компаниями в разработке прогностической полицейской программы. Например, Департамент полиции Ванкувера разработал свою систему GeoDASH в партнёрстве с Latitude Geographics, а полицейская служба Торонто изучила сотрудничество с Environics Analytics в своих решениях для управления полицией на основе данных.

Хотя международные обязательства в области прав человека в первую очередь возлагаются на государства, предприятия также несут ответственность за соблюдение прав человека в соответствии с руководящими принципами Организации Объединённых Наций по предпринимательству и правам человека («руководящие принципы»). [1032] Эти обязанности не зависят от обязательств предприятий по внутреннему законодательству дополняют их. Руководящие принципы устанавливают передовую практику для предприятий, а также определяют обязательства правительств по привлечению предприятий к ответственности за нарушения прав человека, вызванные их деятельностью. Внутри страны квебекская хартия прав и свобод человека также применяется к частным субъектам и потенциально может послужить основанием для возбуждения иска в связи с нарушениями прав человека, совершенными частными компаниями. [1033]

В контексте алгоритмической политики эти обязательства означают, что частные субъекты, такие как Palantir Technologies, Environics Analytics, NEC Corporation, IBM, ShotSpotter, Clearview AI и другие, несут международную нормативную ответственность за оценку продемонстрированного и потенциального воздействия их предпринимательской деятельности на права человека. Компании должны проявлять чуткость к тому, как их деятельность может повлиять на права человека маргинализированных и уязвимых групп населения. К таким группам населения относятся «коренные народы; женщины; национальные или этнические, религиозные и языковые меньшинства; дети; инвалиды; трудящиеся мигранты и члены их семей». [1034] Выполнение этих обязанностей потребует от компаний должной осмотрительности в отношении их потенциального воздействия на права человека. [1035]Должная осмотрительность включает консультации с расовыми и другими непропорционально криминализированными общинами[1036] и устраняет неблагоприятных последствий для прав человека, вызванных их технологиями

[1032] United Nations Human Rights Office of the High Commissioner, «Guiding Principles on Business and Human Rights: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework,» A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/ Publications/GuidingPrinciplesBusinessHR_EN.pdf>.
[1033] Charter of Human Rights and Freedoms, RSQ, c C-12.
[1034] United Nations Human Rights Office of the High Commissioner, «Guiding Principles on Business and Human Rights: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework,» A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/ Publications/GuidingPrinciplesBusinessHR_EN.pdf> at page 14.
[1035] Ibid, at pages 17-19.э
[1036] Ibid, at page 19.

и услугами, включая последствия для права на неприкосновенность частной жизни и права на равенство и не дискриминацию.[1037]

Комплексное участие частного бизнеса, в частности многонациональных технологических компаний, в выполнении традиционных государственных функций, таких как охрана правопорядка, также вызывает вопросы, касающиеся корпоративной социальной ответственности и технологической этики. Эти вопросы о последствиях технического прогресса для прав человека послужили мотивом для более широкого культурного дискурса, который ставит под сомнение руководящую силу современного технологического сектора, [1038]движимую как внешними, так и внутренними критиками.[1039]

Хотя деятельность частного сектора не является главным предметом настоящего доклада, в котором основное внимание уделяется алгоритмической полицейской деятельности правоохранительных органов, включая использование ими технологий частного сектора, авторы отмечают повсюду, где участие частного бизнеса особенно заметно для данной проблемы. Кроме того, эти компании и их потенциал пагубно сказаться на способности отдельных лиц и маргинализированных общин осуществлять свои гарантированные права человека требуют дальнейших исследований в их собственном праве.

[1037] Ibid, at pages 20-21.

[1038] See e.g., Alexis Madrigal, «The Coalition Out to Kill Tech as We Know», The Atlantic (4 June 2019) <https://www.theatlantic.com/technology/ archive/2019/06/how-politicians-and-scholars-turned-against-big-tech/591052/> («At a broad ideological level, two things have happened. First, the idea of cyberspace, a transnational, individualistic, largely unregulated, and free place that was not exactly located in any governmental domain, has completely collapsed. Second, the mythology of tech as the carrier of progress has imploded, just as it did for the robber barons of the late 19th century, ushering in the trust-busting era»); ; see also e.g., Casey Newton, «The tech backlash is real, and it's accelerating», The Verge (17 September 2019), <https://www.theverge.com/interface/2019/9/17/20869495/tech-backlash-nyt-rob-walker-antitrust-privacy>; Madhumita Murgia and Siddarth Shrikanth, «How Big Tech is struggling with the ethics of AI», The Financial Times (28 April 2019) <https://www.ft.com/ content/a3328ce4-60ef-11e9-b285-3acd5d43599e>; Margi Murphy, «Facebook removed from S&P list of ethical companies after data scandals», The Telegraph (13 June 2019) <https://www.telegraph.co.uk/technology/2019/06/13/facebook-gets-boot-sp-500-ethical-index/>; Enrique Dans, «Can Employees Force A Company To Be More Ethical?», Forbes (19 June 2018) <https://www.forbes.com/sites/enriquedans/2018/06/19/can- employees-force-a-company-to-be-more-ethical/#4e78a19e27e3>; Darrel M. West, «The role of corporations in addressing AI's ethical dilemmas», Brookings (13 September 2018) <https://www.brookings.edu/research/how-to-address-ai-ethical-dilemmas/>.

[1039] See e.g., Daisuke Wakabayashi and Scott Shane, «Google Will Not Renew Pentagon Contract That Upset Employees», The New York Times, (1 June 2018) <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>; Julie Carrie Wong, «'We won't be war profiteers': Microsoft workers protest $480m army contract», The Guardian (22 February 2019) <https://www.theguardian.com/technology/2019/ feb/22/microsoft-protest-us-army-augmented-reality-headsets>; Samantha Maldonado, «U.S. tech industry becomes hotbed for employee activism», The Globe and Mail (25 August 2019) <https://www.theglobeandmail.com/business/technology/article-us-tech-industry-becomes- hotbed-for-employee-activism/>; see also Emily Birnbaum, «Over 1,000 students across 17 colleges pledge not to work at Palantir over ICE work», The Hill (16 September 2019) <https://thehill.com/policy/technology/461573-over-1000-students-across-17-colleges-pledge-not-to-work-at-palantir-over>.

5.2 Право на конфиденциальность

Технологии алгоритмической полиции обеспечивают право на неприкосновенность частной жизни в результате методов сбора, обработки и раскрытия данных, на которые эти технологии опираются для того, чтобы делать выводы и прогнозировать или раскрывать информацию о физических лицах. Результаты исследований, приведённых в части 4, свидетельствуют о том, что канадские правоохранительные органы начинают применять различные виды алгоритмических полицейских технологий и, возможно, решат расширить их использование в будущем. Защита частной жизни должна быть интегрирована на переднем крае существующих и будущих инициатив, поскольку возможности сбора и обработки данных, связанные с технологией алгоритмической полиции, могут угрожать праву общественности на защиту от вторжений в частную жизнь. Без адекватных ограничений и надзора, гарантирующих, что любое использование такой технологии необходимо и соразмерно законным целям, неконтролируемые полномочия по использованию алгоритмических полицейских технологий рискуют оставить людей с незаконно ослабленными правами на неприкосновенность частной жизни - никогда не зная, когда и в какой степени государство контролирует и регистрирует их.

Неприкосновенность частной жизни является одним из основных прав человека,[1040] признанных во Всеобщей декларации прав человека и американской Декларации прав и обязанностей человека («Боготская декларация», охватывающая Северную и Южную Америку),[1041] и она защищена в таких международных документах, как Международный пакт о гражданских и политических правах[1042] (ICCPR) и Конвенции о правах ребёнка.[1043] Это право имеет важнейшее значение для человеческого достоинства и автономии и является основополагающим в свободном и демократическом обществе. [1044] Уединение «даёт нам возможность быть самими собой без осуждения, позволяет нам свободно мыслить без дискриминации и является важным элементом предоставления нам контроля над тем, кто знает, что о нас.» [1045]

[1040] Universal Declaration of Human Rights, adopted December 10, 1948, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948), art 12.

[1041] Inter-American Commission on Human Rights (IACHR), American Declaration of the Rights and Duties of Man, 2 May 1948, adopted by Canada in 1948, art 5.

[1042] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 17.

[1043] Convention on the Rights of the Child (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, ratified by Canada 1991, <https://www.ohchr.org/en/professionalinterest/pages/crc. aspx>, art 16.

[1044] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 11.

[1045] Privacy International, «What is Privacy», <https://privacyinternational.org/explainer/56/what-privacy>.

Две всеобъемлющие особенности правовой защиты частной жизни наиболее уместны при оценке алгоритмической полицейской технологии. Во-первых, канадское и международное право прав человека обеспечивают защиту зоны частной жизни. Верховный комиссар ООН по правам человека (УВКПЧ) определил неприкосновенность частной жизни как «презумпцию того, что люди должны иметь область автономного развития, взаимодействия и свободы», которая свободна от вмешательства государства.[1046] В канадском законодательстве охраняемая зона частной жизни определяется желательно, поскольку эта зона связана с тем, что люди должны иметь право ожидать.

Зона приватности не зависит от искусственных различий между публичным и частным пространствами,[1047] публичной и частной информацией. [1048]

Это право должно применяться таким образом, чтобы оно было одинаково значимым для всех людей, особенно с учётом уязвимости, с которой сталкиваются конкретные общины (например, расовые, социально-экономические обездоленные или иным образом исторически маргинализированные группы). [1049]УВКПЧ и Верховный Суд Канады признали, что защита конфиденциальности информации, которая охватывает информацию о человеке и его жизни, особенно важна в современном цифровом обществе. [1050]

Во-вторых, конституционные гарантии и МПГПП запрещают необоснованное вторжение в частную жизнь со стороны правоохранительных органов или правительства. Согласно МПГПП, вмешательство государства в частную жизнь должно быть санкционировано достаточно точным законом и

[1046] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights»(3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 5; see also, United Nations General Assembly, «Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin» (28 December 2009) A/HRC/13/37 <https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> at para 11.

[1047] R v Wise, [1992] 1 SCR 527; R v Jarvis, 2019 SCC 10.

[1048] R v Spencer, [2014] 2 SCR 212 at para 38; Комитет ООН по правам человека выразил обеспокоенность по поводу того, что государственные власти рассматривают все данные, собранные в "общественных зонах", как свободно доступные и общедоступные. See: United Nations Human Rights Committee, «Concluding observations on the seventh periodic report of Colombia» (17 November 2016) CCPR/C/COL/Co/7 <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fCOL%2fCO%2f7&Lang=en> at para 32.

[1049] Органы международного права и эксперты признали, что маргинализированные группы и группы меньшинств особенно уязвимы для государственного надзора и нарушений неприкосновенности частной жизни. See e.g., United Nations General Assembly, Human Rights Council, «Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression» (17 April 2013) A/HRC/23/40 <https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/ Session23/A.HRC.23.40_EN.pdf> at para 51; and United Nations, General Assembly, Committee on Social, Humanitarian and Cultural Issues, «The Right to Privacy in the Digital Age» (16 November 2016) A/C.3/71/L.39/Rev.1 <https://undocs.org/A/C.3/71/L.39/Rev.1>.

[1050] R v Spencer, [2014] 2 SCR 212 at para 40; UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 5-7.

должно быть необходимым и соразмерным достижению законной цели, которая является целью вторжения.[1051] В разделе 8 Хартии также признается, что посягательства на частную жизнь со стороны правоохранительных органов или правительства наносят особый ущерб свободному и демократическому обществу.[1052]

В этом разделе 5.2 («Право на конфедиальность») излагается, как алгоритмическая полиция задействует право на частную жизнь четырьмя ключевыми способами. Во-первых, существуют проблемы конфиденциальности, связанные со сбором данных, которые часто связаны с алгоритмической полицией (раздел 5.2.1). Во-вторых, консолидация и обработка этих данных может привести к алгоритмическим выводам и результатам, которые подразумевают права на неприкосновенность частной жизни и усиливают необходимость надзора (раздел 5.2.2). Дополнительные проблемы могут возникнуть при обмене данными между правоохранительными органами, другими государственными органами и частным сектором (раздел 5.2.3). Наконец, создание или использование неточных данных может привести к возникновению дополнительных проблем конфиденциальности (раздел 5.2.4). Вывод, вытекающий из этого анализа, состоит в том, что технологии алгоритмической полиции потенциально угрожают защищённым интересам конфиденциальности значимыми и новыми способами. Эта потенциальная угроза усиливает необходимость установления ограничений на то, как правоохранительные органы могут использовать технологии, чтобы их использование было пропорционально интересам конфиденциальности, поставленным на карту, и регулировалось независимым и значимым надзором.

5.2.1. Сбор данных: массовое наблюдение и общественное пространство

Многие методы алгоритмической политики основаны на агрегировании и анализе больших объёмов данных, таких как личная справочная информация, коммуникационные данные, биометрические данные, данные геолокации или данные социальных сетей. В то время как правоохранительные органы могут уже обладать некоторой информацией или наборами данных, используемыми алгоритмическими технологиями, методы алгоритмического наблюдения, рассмотренные в части 4, как правило, опираются на систематический сбор новых данных и позволяют это делать. Новые методы сбора данных получают

[1051] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights» (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at paras 23, 25 and 28. See also «The International Principles on the Application of Human Rights to Communications Surveillance», (September 2013) <https://necessaryandproportionate.org/principles>.

[1052] R v Dyment, [1988] 2 SCR 417; see also Schreiber v Canada (Attorney General), [1998] 1 SCR 841.

данные из онлайновых или физических сред, которые, по мнению правоохранительных органов, не защищены правом на частную жизнь. [1053] На самом деле утверждения правоохранительных органов о том, что информация каким-то образом является общедоступной или свободно доступной для их использования в правоохранительных целях, являются спорными и часто утверждаемыми, поскольку до сих пор не существует специального технологического закона, который либо разрешает, либо запрещает сбор данных в первую очередь.

В этом разделе особое внимание уделяется данным, собранным из мест, которые правоохранительные органы часто утверждают или предполагают, что они не защищены в соответствии с Уставом и международным правом прав человека. Эти места будут описаны как «общественные места» для целей настоящего анализа. В этом разделе показано, как технологии алгоритмического наблюдения могут вмешиваться в частную жизнь человека и, следовательно, нарушать раздел 8 Хартии и право на частную жизнь, когда эти технологии используются правоохранительными органами в отсутствие судебного надзора или ограничений, определённых необходимостью и соразмерностью.

Использование правоохранительными органами сложных технологий наблюдения «для дальновидных, «рыболовных экспедиций в надежде обнаружить доказательства преступления»»,[1054] как правило, создаёт острые конституционные и международные проблемы в области прав человека. Три основных фактора разъясняют, почему необходимы гарантии, когда речь заходит об алгоритмических методах наблюдения, основанных на систематическом сборе данных из публичных мест:

1. Сбор данных правоохранительным органом, в частности, в отличие от гражданского члена общественности, влечёт за собой чёткие требования надзора в соответствии с законом о конфиденциальности;

2. Наличие новых, сложных методов анализа данных усиливает последствия конфиденциальности, создаваемые сбором данных;

3. Хартия и право прав человека защищают конфиденциальность как анонимность.

[1053] Технологии алгоритмического наблюдения, которые автоматизируют сбор данных, как правило, полагаются на данные, найденные в общественных местах, как и другие типы м етоды сбора данных, как правило, уже подпадают под действие режима ордера и производственного заказа в Канаде, так что сбор данных не может быть автоматизирован без нарушения установленных в разделе 8 принципов и законов.

[1054] R vJones, [2017] 2 SCR 696, at para 74, citing R v Finlay (1985), 23 CCC (3d) 48 (Ont CA), at p 70; UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights» (30 June 2014) A/HRC/27/37 <https:// undocs.org/A/HRC/27/37>, at paras 23, 25, and 28; UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 35 and 39.

Сбор данных правоохранительными органами отличается в соответствии с законом о конфиденциальности: отдельные лица сохраняют уникальное ожидание конфиденциальности от правоохранительных органов. Это ожидание означает, что люди сохраняют право на защиту своей конфиденциальности от правоохранительных органов, даже если информация уже была раскрыта или обнародована для других целей субъектам, не имеющихся правоохранительными органами.[1055] Хотя отдельные лица неизбежно теряют некоторую степень контроля над своей личной информацией, когда она передается другим, они могут разумно ожидать, что информация не будет передана правоохранительным органам (или собрана ими). [1056]

Право на сохранение защиты информации, которая уже была передана третьей стороне для ограниченных целей, вытекает из того факта, что «вся информация о человеке является фундаментальной [их] собственностью, чтобы [они] могли передавать или сохранять для [себя] по своему усмотрению». [1057]

«Конституционная защита (частично) общедоступной личной информации людей согласуется с тем, как государственные и частные агентства регулируются законодательством о конфиденциальности в Канаде. Например, в 2013 году Управление уполномоченного по вопросам конфиденциальности постановило, что государственный мониторинг и сбор личной информации с личной страницы в Facebook Синди Блэксток, известного борца за права коренных народов, нарушает Закон о конфиденциальности. Закон о конфиденциальности ограничивает сбор личной информации, «независимо от того, доступна ли она публично или нет». [1058]

Доступность более продвинутых методов анализа данных повышает интересы конфиденциальности участие в сборе данных: анализ того, мешают ли методы сбора данных правоохранительными органами частной жизни людей, требует оценки того, что раскрывает информация о частной жизни людей и как правоохранительные органы могут использовать эти данные. Если рассматривать изолированно, некоторые типы общедоступных личных данных могут не раскрывать конфиденциальную или личную информацию. Например,

---

[1055] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 6. The OHCHR has also stated that data sharing between law enforcement agencies and other state agencies risks violating privacy rights «because surveillance measures that may be necessary and proportionate for1972)

[1056] Rv Wise (1992) 1 SCR 527: R v Cole. 2012 SCC 3.R v Marakah. 2017 SCC 59: R vjones. 2017 SCC 60.

[1057]UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 7, 20.. 1972) at p 13; UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights» (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 7, 20.

[1058] Office of the Privacy Commissioner of Canada, «Aboriginal Affairs and Northern Development Canada wrongly collects information from First Nations activist's personal Facebook page» (29 October 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/ investigations-into-federal-institutions/2012-13/pa_201213_01>.

отдельная публикация в социальных сетях или данные о геолокации автомобиля в определенный момент времени относительно менее открыты, чем другие типы конфиденциальных данных, такие как медицинские записи или то, что передается в индивидуальных текстовых сообщениях или телефонных разговорах.

Однако, когда личная информация собирается систематически, чтобы её можно было связать и проанализировать с помощью технологий алгоритмического наблюдения, последствия практики сбора данных для конфиденциальности могут быть значительными.[1059]Агрегирование и алгоритмический анализ данных потенциально может раскрыть подробную картину о лицах, которых они не ожидают, не говоря уже о том, чтобы ожидать, что они будут иметь правительство. Действительно, создание этого более детального портрета частной жизни человека даёт основание для использования инструментов на основе алгоритмического наблюдения - они собирают и раскрывают информацию, которая иначе была бы недоступна правоохранительным органам.[1060]

Хартия и закон о правах человека защищают конфиденциальность как анонимность: методы алгоритмического наблюдения потенциально могут подорвать защищенные формы анонимности в общественной жизни. Верховный суд Канады признал, что «некоторая степень анонимности является признаком большой активности в Интернете», [1061]когда постановил, что правоохранительные органы должны иметь ордер на получение информации о подписчике IP-адреса. Люди зачастую мало знают о масштабах своего электронного следа (и о том, в какой степени электронная деятельность вообще создает записи), и они могут быть ещё менее осведомлены о том, как анонимность их электронного следа может быть подорвана или уничтожена современными методами обработки данных. Агрегирование и анализ метаданных и других электронных записей с открытым исходным кодом без судебного надзора может обеспечить сомнительный доступ к информации, которую, как заявил Верховный суд, нельзя получить прямыми способами. Гарантии конфиденциальности, включая предварительное судебное разрешение, необходимы, когда правоохранительные органы собирают и анализируют контент и метаданные, полученные с онлайн-платформ или

[1059] R v Rogers Communications, 2016 ONSC 70; UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights» (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37> para 19.

[1060] Этот сценарий предполагает, что собранные данные и созданный профиль человека точны и не искажены предвзятостью или ошибками. Г де такие данные или полученный профиль неточны, речь идет не только о правах на конфиденциальность пострадавшего (из-за исходных данных но они также могут быть подвергнуты другим видам вреда, которые нарушают другие их права человека, например, незаконно задержаны или арестованы, thus violating their rights to liberty and to be free from arbitrary detention.

[1061] R v Spencer, [2014] 2 SCR 212 at para. 48.

других сред, где отдельные лица действуют свободно с относительной анонимностью.

Методы наблюдения за социальными сетями описанны в разделе 4.3 («Инструменты алгоритмического наблюдения») и освещены вышеупомянутые три причины, по которым такие технологии необходимо сдерживать с помощью контроля и ограничений, обеспечивающих необходимость и соразмерность использования. RCMP занял позицию, согласно которой они могут использовать онлайн-наблюдение в социальных сетях, потому что эта форма наблюдения опирается на данные из открытых источников или общедоступных данных.[1062] Однако позиция RCMP представляет собой чрезмерное упрощение поставленных на карту интересов конфиденциальности. Во-первых, когда люди используют социальные сети, они не ожидают, что их информация будет систематически собираться правоохранительными органами.[1063] Во-вторых, платформы социальных сетей содержат огромное количество информации об интимной жизни людей, личных отношениях и повседневной деятельности, которая обычно не предоставляется пользователями в правоохранительных целях. Профессор Тереза Скасса указала, что полиция часто получает доступ к этой информации способами, которые не предупреждают пользователей о том, что они находятся под наблюдением или что их данные используются в полицейском расследовании.[1064] Как отмечалось в разделе 4.2 («Алгоритмическая политика, ориентированная на человека»), SPPAL указала, что намеревается начать сбор данных социальных сетей, чтобы задействовать свою технологию алгоритмической полицейской проверки, ориентированную на человека, причём некоторые такие коллекции потенциально включают данные социальных сетей, полученные от уязвимых лиц, таких как несовершеннолетние. Интересы конфиденциальности, поставленные на карту, ещё больше усиливаются, когда данные социальных сетей систематически собираются с течением времени и анализируются для создания ещё более откровенной картины личности. В-третьих, участие в социальных сетях в Интернете является примером свободы, которую даёт анонимность в публичном онлайн-пространстве .

В окружающей среде активность происходит в «ситуационном ландшафте», [1065]в котором люди не ожидают систематического наблюдения,

---

[1062] Bryan Carney, «'Project Wide Awake': How the RCMP Watches You on Social Media», The Tyee (25 March 2019) <https://thetyee.ca/ News/2019/03/25/Project-Wide-Awake/>.

[1063] R v Spencer, [2014] 2 SCR 212 at para 38-50: «[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public.»

[1064] Teresa Scassa, «Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges» (December 2017) 14:2 Scripted 239 at 251, <https://script-ed.org/wp-content/uploads/2017/12/scassa.pdf>.

[1065] R v Wise, [1992] 1 SCR 527.

подобно тому, как они ожидают возможности слиться с толпой. Пока люди могут знать, что их профили в социальных сетях находятся в открытом доступе, из этого не следует, что они ожидают, что полицейские службы будут систематически наблюдать.

Учитывая потенциальные интересы конфиденциальности, которые проявляются, когда правоохранительные органы проводят массовый сбор данных, ключевой вопрос, который возникает из раздела 8 Хартии и международного права прав человека, заключается в том, будет ли упреждающий сбор данных в надежде на прогнозирование потенциальных преступлений или для получения общей информации сбор либо необходим, либо соразмерен.[1066] Раздел 8 обычно требует, чтобы всякий раз, когда правоохранительные органы вторгаются в защищенную сферу частной жизни, у них должны быть разумные основания полагать, что запрошенная информация обнаружит доказательства преступления.[1067] Превентивные рыболовные экспедиции вряд ли могли удовлетворить этот стандарт. При толковании стандартов Устава следует повторить, что принципы необходимости и соразмерности являются пробными камнями в применении многих частных и государственных секторов закона о конфиденциальности.[1068]

Судебный надзор должен также регулировать сохранение общественных интересов, когда правоохранительные органы стремятся полагаться на алгоритмические технологии наблюдения.[1069] Верховный комиссар ООН по правам человека призвал к участию всех ветвей власти в осуществлении надзора за программами надзора в дополнение к судебному надзору, а также к созданию независимых гражданских надзорных органов. [1070] Надёжный надзор за использованием алгоритмических технологий наблюдения, как минимум, необходим для обеспечения уверенности общественности в том, что

[1066] R vJones, [2017] 2 SCR 696 at para 74, citing R v Finlay (1985), 23 CCC (3d) 48 (Ont CA), at p 70.

[1067]R v Rogers Communications, 2016 ONSC 70. There are, of course, context-specific exceptions to this general proposition where the public interests at stake may warrant a departure from this principle (such as various exigent circumstances relating to public safety and destruction of evidence).

[1068] Например, Апелляционный суд Онтарио в 2007 году постановил, что подзаконный акт, требующий от ломбардов сообщать имена всех клиентов продажа товаров в магазин была недействительна в соответствии с MFIPPA. Это включало постановление о том, что сбор не был оправдан с точки зрения правоохранительных органов, поскольку «передача [данных] происходит до того, как появятся какие-либо основания подозревать, что товары, которые были проданы ... были украдены, и осуществляется без ограничений в отношении их использование полицией или теми, кому полиция может передать информацию Cash Converters v Oshawa, 2007 ONCA 502, at para38.

[1069] Hunter v Southam, [1984] 2 SCR 145; R v Tse, 2012 SCC 16; R vJones, [2017] 2 SCR 696, at para 74; UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights» (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 37.

[1070] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights» (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 37. Дополнительный надзор был принят, например, в законодательных поправках к Уголовному кодексу в 1970-х годах, которые регулируют перехват частных сообщений. В целях усиления мер по обеспечению подотчетности министр общественной безопасности и готовности к чрезвычайным ситуациям по закону обязан готовить и представлять парламенту ежегодный доклад об использовании перехватов и прослушивания телефонных разговоров (Уголовный кодекс, статья 195).

использование правоохранительными органами алгоритмических средств является разумно обоснованным, необходимым и соразмерным. В тех случаях, когда правоохранительные органы стремятся использовать упреждающую практику сбора данных, эта практика противоречит этому давно установленному принципу, согласно которому действия полиции, вторгающиеся в охраняемые формы частной жизни, подлежат значительному надзору.

5.2.2. Обработка данных: анализ данных и алгоритмические выходы

В связи со сбором и обработкой данных правоохранительными органами возникают проблемы, связанные с конфиденциальностью, но отличающиеся друг от друга. В то время как раздел 5.2.1 («Сбор данных: массовое наблюдение и общественное пространство») рассматривает последствия для конфиденциальности, связанные с методами сбора данных и технологией алгоритмического контроля, в другом разделе (раздел 5.2.2) основное внимание уделяется деятельности правоохранительных органов, включающей обработку и анализ информации, уже контролируемой правоохранительными органами. Действия по обработке данных затрагивают уникальные интересы конфиденциальности и, следовательно, должны быть необходимыми, целесообразными и служить законной цели.[1071]

Аналитика данных может дать представление о людях и их личности, движениях, интересах, убеждениях и социальных сетях. Такие идеи извлекаются не только из данных, но и из метаданных – информации о телефонных звонках, электронных письмах, сообщениях в социальных сетях и других коммуникациях, помимо содержания сообщений (например, время, дата, местоположение, отправитель или получатель), – которые могут привести к заключениям о частной жизни людей при агрегировании и анализе.[1072]

Алгоритмы распознавания образов могут извлекать информацию о защищаемых характеристиках, таких как раса или этническая принадлежность, религиозные убеждения, возраст, пол и сексуальная ориентация, даже если эти данные не включены в исходные наборы данных.[1073]Таким образом, права на

[1071] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 29; Re (X), 2016 FC 1105 at paras 79 and 265.

[1072] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 19; Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017), at 119-120. <https://www.priv.gc.ca/en/opc-actions-and- decisions/research/explore-privacy-research/2014/md_201410/>; R v Rogers Communications, 2016 ONSC 70; R v Spencer, [2014] 2 SCR 212.

[1073] См. обсуждение прокси-данных в разделе 5.4.2 ("Алгоритмическое смещение и" Контуры обратной связи

конфиденциальность относятся не только к собираемым данным, но и к выводам, сделанным из объединённых фрагментов данных, и к результатам алгоритмической обработки.[1074]

Более многочисленные и подробные выводы, которые могут возникнуть в результате более высоких технологических возможностей алгоритмического анализа, усиливают интересы конфиденциальности.[1075] Многие полицейские базы данных появились раньше алгоритмических технологий и, как обсуждалось в разделе 2.2. («Предвзятость и неточность в данных полиции»), могут содержать данные, которые не подходят для работы с такими технологиями. Принимая во внимание такие опасения, представитель SPPAL отметил, что их команда рассматривала возможность использования машинного обучения для создания наборов синтетических данных; эти наборы данных затем будут использоваться для тестирования своих алгоритмических моделей и моделирования результатов корректировки различных переменных.[1076]Теоретически это позволит SPPAL снизить потребность в использовании данных реальных людей и снизить риски, связанные с конфиденциальностью. Однако, даже синтетические наборы данных могут вызывать проблемы с конфиденциальностью из-за потенциальной необходимости использовать реальные данные для обучения алгоритма, чтобы он мог генерировать полезные синтетические наборы данных.[1077]

В то время как раздел 8 наиболее четко регулирует сбор информации правоохранительными органами, требуя от агентов получения ордера на обыск до проведения обысков и выемок в рамках уголовных расследований, конституционные гарантии в соответствии с разделом 8 также защищают

несправедливости "), включая примеры того, как алгоритмы использовались для вывода расовых, гендерных и медицинских условий из таких данных, как почтовые индексы, условия онлайн-поиска," лайки "Facebook и история покупок. См. также Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 34 («AI methods on social media platforms are used to infer and generate sensitive information about people that they have not provided or confirmed, such as sexual orientation, family relationships, religious views, health conditions, or political affiliation").

[1074] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 30.

[1075] Например, сотрудники правоохранительных органов часто привлекаются для участия в мероприятиях, связанных с жалобами на уголовные преступления, но и они тоже вызваны на такие события, которые вполне могут попасть в полицейскую базу данных, однако далеко не ясно, какая законная цель правоохранительных органов позволит службам использовать личные данные для алгоритмов распознавания образов или других алгоритмических оценок. См. также общественный резонанс, возникающий, когда люди узнали, что их фотографии и изображения, общие в одном контексте, были перепрофилированы для использования в учебных наборах данных для алгоритмов распознавания лиц: Olivia Solon, «Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", NBC News (12 March 2019) <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

[1076] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

[1077] See e.g., Information and Privacy Commissioner for British Columbia, «Investigation Report P19-01: Full Disclosure: Political parties, campaign data, and voter consent", (6 February 2019) <https://www.oipc.bc.ca/investigation-reports/2278> at 25-26 (regarding Facebook's «Lookalike" feature).

интересы конфиденциальности, которые возникают при использовании изъятой информации.[1078] Короче говоря, защита раздела 8 может быть задействована технологиями алгоритмического контроля, основанными на том, как они обрабатывают собранные данные. Например, использование полицейскими службами систем распознавания лиц для идентификации изображений неизвестных лиц создает проблемы конфиденциальности, которые отличаются при наличии у служб баз данных с фотографиями из кружков. Точно так же технология ALPR создает уникальные проблемы с конфиденциальностью во время её использования по сравнению с записью местоположения и номерного знака человека в полицейской записной книжке. В обоих случаях повышенный интерес возникает из-за комбинации существующих ставок на конфиденциальность и более совершенных возможностей наблюдения и анализа данных, используемых правоохранительными органами.[1079]Таким образом, хотя большая часть юриспруденции раздела 8 сосредоточена на регулировании сбора данных, от судов и регулирующих органов конфиденциальности, вероятно, будет всё больше и больше требоваться рассмотрение того, какие меры предосторожности необходимы в случае, когда правоохранительные органы будут использовать алгоритмические инструменты для обработки собранной информации в целях получения информации о людях и их предполагаемой деятельности.

5.2.3. Обмен данными: государственные органы и частные компании

Наблюдение и сбор данных, которые необходимы и соразмерны одной законной цели, могут не подходить для другой. [1080] В 2012 году комиссар

[1078] R v Reeves, 2018 SCC 56; Wakeling v. United States of America, 2014 SCC 72.

[1079] Например, Комиссар по вопросам информации и конфиденциальности Британской Колумбии установил, что любое последующее использование "незащищенной" информации, собранной в рамках полицейской программы ALPR, является незаконным в соответствии с применимым законодательством о конфиденциальности: Office of the Information & Privacy Commissioner, «Investigation Report F12-04 - Use of Automated Licence Plate Recognition Technology by the Victoria Police Department" (15 November2012), <https://www.oipc.bc.ca/investigation-reports/1480>. Правоохранительные органы также все чаще получают данные, доступные им через частные сети наблюдения, такие как база данных отслеживания номерных знаков компании Digital Recognition Network (DRN). База данных DRN якобы содержит девять миллиардов сканированных номерных знаков - «краудсорсинг сотнями репозиториев, которые установили камеры, пассивно сканирующие, захватывающие и загружающие номерные знаки каждого автомобиля, на котором они ездят база данных DRN», позволяющая как частным следователям, так и првоохранительным органам отслеживать передвижения владельцев автомобилей в течение длительного времени." Joseph Cox, «This Company Built a Private Surveillance Network. We Tracked Someone With It", VICE Motherboard (17 September 2019) <https://www.vice.com/en_ca/article/ne879z/i-tracked-someone-with-license-plate- readers-drn>.

[1080] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 27; Office of the Privacy Commissioner of Canada, «Canada Border Services Agency - Scenario Based Targeting of Travelers - National Security" (2017) <https://www.priv.gc.ca/en/opc-actions- and-decisions/audits/ar-vr_cbsa_2017/>; Office of the Information & Privacy Commissioner, «Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>; Re (X), 2016 FC 1105; Wakeling v. United States of America, 2014 SCC 72. В целом в соответствии с Уголовным кодексом и соответствующим законодательством о неприкосновенности частной жизни многие случаи ареста,

Британской Колумбии по информации и конфиденциальности обнаружил, что правоохранительные органы использовали технологии распознавания лиц и фотографий водительских прав, принадлежащих государственной автомобильной страховой компании провинции, что нарушило провинциальное законодательство о конфиденциальности. [1081] Государственный страховщик не мог разрешить использование своей базы данных для целей, о которых не было известно клиентам, [1082] таким образом, правоохранительным органам было запрещено в соответствии с законодательством использовать базу данных водительских прав в качестве полицейского инструмента без разрешения суда.[1083]Ориентированное на человека прогнозирование зависит от построения подробного профиля человека путем объединения различных типов данных и информации о них для оценки потенциального будущего поведения или риска. Один из способов получения полицейскими службами данных, к которым они могут не иметь доступ – это сбор их у других организаций, включая частные компании и государственные органы, которые собрали данные для своих собственных целей.

Как вы отслеживаете, что делают с данными? Например, при кардинге [полицейскими службами] люди очень озабочены тем, что они делают с данными. Где передаются данные? У кого ещё есть доступ? – Центр судебных исков чернокожего населения (Black Legal Action Centre (BLAC)[1084]

Хаб-модель контроля (см. в фокусе № 3: Хаб-модель общественной безопасности) служит примером проблем конфиденциальности, связанных с обменом данными между правоохранительными органами и другими сторонними субъектами. Эта модель представляет собой программу оценки рисков, которую можно рассматривать как своего рода предшественника алгоритмической полицейской технологии. Модель Hub объединяет сотрудников школы, агентства социальных услуг, поставщиков медицинских услуг и полицейские службы для обмена информацией о лицах, которые, как

санкционированные судом, затрудняют хранение полученной информации и обмен ею. Например, часть VI Уголовного кодекса квалифицирует в качестве уголовного преступления обмен перехваченными сообщениями, если это не разрешено Кодексом.

[1081] Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

[1082] Office of the Information & Privacy Commissioner, «Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

[1083]Там же. На момент проведения расследования Уполномоченный по вопросам информации и неприкосновенности частной жизни установил, что в 2011 - 2012 годах страховщик получил 15 просьб непосредственно от полицейских сил об оказании помощи в установлении личности физических лиц, и по крайней мере в одном случае страховщик предоставил полиции возможную личность физического лица на основе только просьбы полиции; для раскрытия не требовалось ордера или повестки в суд: Office of the Information & Privacy Commissioner, «Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>, at para 96.

[1084] Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

считается, находятся в группе риска. [1085] Информация, собранная в базах данных Hub, обычно чрезвычайно чувствительна.

Она включает возрастную группу, пол, местонахождение человека и более сотни факторов, таких как предполагаемые проблемы с психическим здоровьем, употребление алкоголя и наркотиков, «отрицательные сверстники», неприятное или деструктивное поведение, пропуск школы, физическое здоровье и бедность, которые предположительно указывают риск.[1086] Практика совместного использования данных в модели Hub способствует созданию баз данных отслеживания рисков, которые доступны и используются правоохранительными органами. Такое использование включает оценку и анализ информации базы данных с использованием алгоритмических методов, таких как те, которые в настоящее время разрабатываются в SPPAL.[1087] Эти программы порождают конституционные проблемы и проблемы с конфиденциальностью, несмотря на попытки встроить фильтры конфиденциальности, предназначенные для проверки данных на различных этапах для определения уровней совместного использования и устранения опасений по поводу конфиденциальности в связи с ненадлежащим обменом или использованием информации.[1088] Например, комиссар Саскачевана по информации и конфиденциальности обнаружил, что меры по деидентификации в программе Hub в Саскачеване были недостаточными.[1089] Более того, систематический обмен данными с правоохранительными органами имеет конституционные разветвления, а именно потенциальное нарушение прав, предусмотренных разделом 8, с учётом возможности правоохранительных органов получать доступ к личным данным отдельных лиц через Хаб без таких гарантий, как предварительное судебное разрешение. Закон уже является потенциальным средством защиты: участники программы Hub связаны более

[1085] Nathan Munn, «Canada's 'Pre-Crime' Model of Policing Is Sparking Privacy Concerns", VICE Motherboard (19 January 2017) <https://www.

[1086] Nathan Munn, «Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database", VICE Motherboard (27 February 2019) <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>.

[1087] Nathan Munn, «Canada's 'Pre-Crime' Model of Policing Is Sparking Privacy Concerns", VICE Motherboard (19 January 2017) <https://www. vice.com/en_us/article/mg7w4x/canada-hub-and-cor-policing-privacy-police>; Nathan Munn, «Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database", VICE Motherboard (27 February 2019) <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking- peoples-negative-behavior-in-a-risk-database>.

[1088] Сторонние агентства должны самостоятельно соблюдать действующее законодательство о конфиденциальности, которое регулирует сбор, хранение, использование и раскрытие личной информации или личной медицинской информации. Верховный комиссар Организации Объединенных Наций по правам человека предложила установить "ограничения использования" для контроля за обменом данными между правоохранительными и другими государственными органами, поскольку информация, собранная для одной цели, может быть не необходимой и соразмерной для другой (UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at paras 26-27). This section instead looks at what obligations may arise under the Charter where such third parties interact with law enforcement entities in a manner such that their conduct gives rise to Charter rights or violations.

[1089] Saskatchewan Information & Privacy Commissioner, «Investigation Report 105/2014: Community Mobilization Prince Albert" (10 November 2014) <https://oipc.sk.ca/assets/foip-investigation-105-2014.pdf>, at pages 11-18.

строгими обязательствами Хартии при определенных обстоятельствах.[1090] Не полицейские субъекты иногда могут стать полицейскими агентами, которые связаны теми же конституционными ограничениями, что и правоохранительные органы, в отношении сбора или изъятия информации.[1091] В частности, если субъекты, не являющиеся правоохранительными органами, ищут или изымают личную информацию по запросу правоохранительных органов, меры защиты по разделу 8 применяются к действиям полицейского агента (включая необходимость получить предварительное судебное разрешение).[1092]

Эти гарантии применяются к полицейскому агенту, поскольку органы уголовной полиции государства не могут полагаться на изъятие частных данных другими государственными субъектами для обхода гарантий, предусмотренных в разделе 8.[1093]

Даже если агентские отношения между полицией и субъектами, не относящимися к полиции, не возникают, если по своей собственной инициативе государственный субъект проводит расследование в целях уголовного законодательства, лица, находящиеся под следствием, снова будут иметь право на те же меры защиты Хартией, которые возникают в ходе полицейского расследования. Эти права, закреплённые в Хартии, включают право хранить молчание, право на адвоката и защиту от необоснованных обысков и арестов. Предварительное судебное разрешение потребуется до того, как государственный агент наложит арест на личные записи того или иного лица и передаст их правоохранительным органам.[1094]

Следовательно, глубокие конституционные последствия возникнут, если персонал государственных служб (например, учителя, социальные работники

[1090] R v Orlandis-Habsburgo, 2017 ONCA 649; R v Pohoretsky, [1987] 1 SCR 945; R v Dersch, [1993] 3 SCR 768 at para 20. Представитель правоохранительных органов в Канаде в ходе исследовательского интервью сообщил, что Hub-столы в Торонто получают большинство своих дел через передачи из полицейской службы Торонто (TPS), предполагая, что многие лица могут быть выведены из правоохранительного контекста и переведены в одно или несколько учреждений социального обслуживания с целью оказания поддержки, в отличие от учреждений социального обслуживания, передающих дела в правоохранительные органы. Интервью представителя правоохранительных органов Канады компании Yolanda Song & Cynthia Khoo (28 июня 2019 года). Однако это не ослабляет озабоченности тех, кто обращается за социальными услугами, и, в конечном счете, вовлекается в систему уголовного правосудия путем направления в центр.

[1091] R v Orlandis-Habsburgo, 2017 ONCA 649; R v Pohoretsky, [1987] 1 SCR 945; R v Dersch, [1993] 3 SCR 768 at para 20; and R v Jarvis, 2002] 3 SCR 757. Кроме того, положения об обязательном удержании третьих сторон не считаются ни необходимыми, ни соразмерными в соответствии с международным правом прав человека в отношении права на неприкосновенность частной жизни, особенно без включения ограничений на то, каким образом сохраненные данные могут впоследствии использоваться. UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at paras 26-27.

[1092] Ibid and R v Orlandis-Habsburgo, 2017 ONCA 649. In some circumstances, the individual who is the subject of «investigation" and faces potential criminal jeopardy may be entitled to other Charter protections such as the right to counsel: R v Jarvis, [2002] 3 SCR 757.

[1093] R v Colarusso, [1994] 1 SCR 20.

[1094] R v Jarvis, [2002] 3 SCR 757.

или поставщики медицинских услуг) будет преобразован в полицейских агентов в соответствии с законом, что может потребоваться Хартии в результате анализа их систематической практики обмена данными с полицейскими службами в рамках программы Hub. Такие механизмы обмена данными могут также подорвать доверие общества к основным социальным услугам и работникам государственных служб или удерживать уязвимых лиц от доступа к таким услугам.[1095]Подобные конституционные проблемы и проблемы конфиденциальности могут возникать с другими инструментами алгоритмического контроля, когда правоохранительные органы стремятся получить доступ к наборам данных, собранным частными компаниями.[1096]Например, полицейская служба Калгари (CPS) использует программное обеспечение от Palantir Technologies, которое может интегрировать коммерческую информацию третьих сторон, такую как финансовые записи, отчеты о доставке, телекоммуникационная информация и телеграфные переводы, с полицейскими базами данных,[1097]хотя, судя по исследовательскому интервью, проведенному в мае 2019 года, похоже, что CPS не использует эти возможности.[1098]Инструменты распознавания лиц, используемые правоохранительными органами, могут использоваться для обработки сделанных изображений.[1099]Эти механизмы обмена информацией уязвимы с точки зрения Конституции, поскольку клиенты, которые могли дать согласие на то, чтобы частный бизнес собирал их изображения в целях обслуживания клиентов, не сделали этого на том основании, что они также давали согласие на обмен своей информацией с полицейскими службами в целях обеспечения правопорядка. [1100]Законодательство о коммерческой конфиденциальности в Канаде, регулируемое федеральными (PIPEDA) и провинциальными органами, также не разрешает раскрытие информации без

[1095] See, for example, R v Pohoretsky, [1987] 1 SCR 945; R v Dersch, [1993] 3 SCR 768 at para 20.

[1096] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 27.

[1097] Calgary Police Service, «Palantir Platform Capabilities Brief" (obtained through freedom of information request 18-G-1921); Calgary Police Service, «Calgary Police Service Palantir Implementation Privacy Impact Assessment", at p 47 (obtained through freedom of information request 18-G-1921).

[1098] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

[1099] Hannah Devlin, «'We are hurtling towards a surveillance state': the rise of facial recognition technology", The Guardian (5 October 2019), https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>. Для примера далеко идущей технологии распознавания лиц, которую правоохранительные органы уже использовали в Соединенных Штатах, разработанной и проданной компанией под названием Clearview AI, see: Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It", New York Times (18 January 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

[1100] Во многих случаях частные предприятия, возможно, не получили необходимого согласия на сбор изображений лица даже для целей, не связанных с правоохранительными органами: Julia Carrie Wong, «Google reportedly targeted people with 'dark skin' to improve facial recognition", The Guardian (3 October 2019), <https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color>.

согласия правоохранительных органов, если только правоохранительные органы не имеют «законных полномочий» для доступа к информации.[1101]

«Законные полномочия» определяются за пределами этого законодательства о конфиденциальности со ссылкой на раздел 8, включая его стандарты для разумных ожиданий конфиденциальности.[1102]Если другие канадские правоохранительные органы разработают инструменты алгоритмического контроля, которые зависят от практики обмена данными между организациями частного сектора и правоохранительными органами, будут затронуты конституционные вопросы. Обмен данными между частными компаниями и правоохранительными органами может сделать деятельность по сбору и обмену данными частной компанией незаконной или неконституционной, независимо от того, происходил ли обмен данными в отдельных случаях или как часть формализованной или рутинной системы обмена с правоохранительными органами.[1103]По сути, правоохранительные органы не могут собирать персональные данные и информацию от частных предприятий, которые сотрудники полиции не могли бы получить напрямую, и любые попытки сделать это могут представлять собой незаконный обход законов о неприкосновенности частной жизни и конституционных законов, которые действуют для защиты граждан от потенциальных злоупотреблений государственной властью. Предоставление правоохранительным органам доступа к данным, которые они не могут получить по Конституции, через частную компанию, получившую данные на законных основаниях, может представлять собой неконституционное расширение возможностей государства по мониторингу и отслеживанию людей без оправдания или судебного надзора.

[1101] See e.g., Personal Information Protection and Electronic Documents Act, RSC 2000, c 5, s 7(3)(c.1).

[1102] R v Spencer, [2014] 2 SCR 212 at paras 60-66, considering the Personal Information Protection and Electronic Documents Act, SC 2000, c 5.

[1103] R v Orlandis-Habsburgo, 2017 ONCA 649 at paras 31-33 and 98-115; R v Cole, 2012 SCC 53; R v Reeves, 2018 SCC 56; R v Spencer, [2014] 2 SCR 212.

5.2. 4.Точность данных: неточные данные и неточные алгоритмы

Точность данных является основным принципом конфиденциальности в международном праве прав человека и канадском законодательстве о конфиденциальности. ICCPR защищает право физических лиц требовать исправления неверных персональных данных, которые собираются или обрабатываются лицами, государственными или частными субъектами.[1104] Внутреннее законодательство о неприкосновенности частной жизни также, как правило, требует от государственных учреждений принятия разумных мер для обеспечения точности данных личной информации, которую они собирают и используют.[1105]

Аналогичные обязательства применяются к частным поставщикам полицейской техники или субъектам частного сектора, которые предоставляют информацию полиции.[1106] Однако права на точность данных не являются единственной проблемой, связанной с неточными данными. Такие неточности могут привести к серьезным ошибкам при обработке с помощью технологий алгоритмического контроля. Нельзя предполагать надежность алгоритмических инструментов до тех пор, пока каждый инструмент не будет независимо и тщательно протестирован, чтобы подтвердить, что он соответствует приемлемому уровню надёжности. В конечном итоге точность входных данных неизбежно повлияет на общую надежность алгоритмического инструмента.

В Канаде полицейские службы регулярно используют информацию, которая может быть неточной, недостоверной или основанной на необъективных обобщениях. Канадский полицейский информационный центр (CPIC), в центральной базе данных которой хранится информация о судимости и к которой имеют доступ правительственные ведомства и правоохранительные органы по всей стране, подвергается широкой критике за устаревание и неточность.[1107] Суд Онтарио отказался, например, принять судебное

[1104] UNHRC, General Comment No 16 on Article 17 (Right to Privacy), 32nd Sess, adopted 8 April 1988, UN Doc HRI/GEN/1/Rev9 (Vol I), at para 10 <https://undocs.org/HRI/GEN/1/Rev.9(Vol.I)>. See also UN Human Rights Council, «The right to privacy in the digital age: Report of call for collected personal data to be accurate, complete, and up-to-date; see Organisation for Economic Co-operation and Development, OECD Guidelines governing the protection of privacy and transborder flows of personal data" (1980, revised in 2013) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, at para 8.

[1105] See, e.g., Privacy Act, RSC 1985, c P-21, s 6(1); Freedom of Information and Protection of Privacy Act, RSA 2000, c F-25, s 35 (Alberta); Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165, s 28 (British Columbia); The Local Authority Freedom of Information and Protection of Privacy Act, SS 1990-91, c L-27.1, s 26 (Saskatchewan).

[1106] See Personal Information Protection and Electronic Documents Act, SC 2000, c 5; and Office of the Privacy Commissioner of Canada, «Accuracy" (May 2013) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic- documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/>.

[1107] Alyshah Hasham, «Criminal-record database spotty and out of date, lawyers lament", The Toronto Star (9

уведомление о надежности базы данных и подтвердил, что ответственность за обеспечение достоверности информации лежит на правительстве, если оно хочет полагаться на нее при посягательстве на свободу человека.[1108]Данные социальных сетей и другая информация из открытых источников могут быть ненадежными, но правоохранительные органы получают к ним доступ без особого надзора.[1109]Молодые люди могут быть помечены в полицейских базах данных как причастные к бандам на основании непроверенной информации, полученной от школьного персонала или местных поставщиков услуг[1110]или на информации, которая может быть основана на предвзятости или предположениях о расе, районе проживания и друзьях.[1111]Сами по себе эти ошибки могут иметь серьезные последствия для прав и жизни людей и их семей.[1112]

Усугубление таких ошибок путем использования алгоритмических средств контроля еще больше увеличивает этот риск, поскольку это ещё больше повышает вероятность того, что данные будут использоваться и обрабатываться правоохранительными органами при принятии решений и проведении расследований.[1113]

Меня беспокоят системы, которые могут быть построены на ограниченных или некорректных данных. – Джонатан Рудин (юрист, автор и программный директор Юридических услуг для аборигенов (Aboriginal Legal Services).[1114]

Несмотря на потенциальные последствия и ущерб, связанные с использованием правоохранительными органами неточных данных в ходе уголовных расследований, некоторые провинции Канады освобождают личные данные, собираемые для правоохранительных целей, от обязательств по

December 2016) <https://www. thestar.com/news/crime/2016/12/09/criminal-record-database-spotty-and-out-of-date-lawyers-lament.html >; Brigitte Bureau, «RCMP database remains out of date, police and prosecutors say", CBC News (10 March 2015) <https://www.cbc.ca/news/politics/rcmp-database-remains-out-of- date-police-and-prosecutors-say-1.2989397>.

[1108] R v White, 2006 ONCJ 147 at para 28.

[1109] Nathan Munn, «Canadian Cops Will Scan Social Media to Predict Who Could Go Missing", VICE Motherboard (17 April 2019) <https://www. vice.com/en_us/article/mb8jzp/canadian-cops-will-scan-social-media-to-predict-who-could-go-missing>; Bryan Carney, «'Project Wide Awake': How the RCMP Watches You on Social Media", The Tyee (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>; Amanda Pfeffer, «Doubts swirl around new Ottawa police nerve centre", CBC News (31 May 2017) <https://www.cbc.ca/news/canada/ottawa/opsoc- ottawa-police-strategic-operations-centre-1.4138242 >; Calgary Police Service, «Internet Investigations and Criminal Intelligence Ref #IN-026", at p 47 (obtained through freedom of information request 18-G-1921).

[1110] Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

[1111] Nathan Munn, «This B.C. city is tackling gang violence by profiling high school students", VICE Motherboard (7 January 2019). <https://www. vice.com/en_ca/article/59vv8x/this-bc-city-is-tackling-gang-violence-by-profiling-high-school-students>.

[1112] See Section 2.1 («Criminal Justice and Systemic Discrimination in Canada"), discussing the impact of criminal justice processes on individuals.

[1113] See Section 2.2 («Bias and Inaccuracies in Police Data»).

[1114] Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019), speaking on behalf of himself only, in a personal capacity.

обеспечению точности данных.[1115] Даже в тех случаях, когда закон устанавливает стандарты точности информации, используемой полицией, неясно, как это требование может быть строго соблюдено. Специалисты по уголовному праву регулярно имеют дело с делами, в которых участвуют лица, на жизнь которых различными способами повлияли ошибки в полицейских записях и базах данных. Во многих случаях к тому времени, когда ошибка обнаруживается и исправляется – часто по инициативе пострадавшего человека – последствия ошибки (ошибок) уже произошли (например, неправомерный арест или обвинение приводит к потере возможности трудоустройства в связи с ошибочной проверкой судимости). Кроме того, мало значимые средства легко доступны. Когда данные передаются в правительстве или между государственными и частными организациями, людям может быть невероятно сложно даже определить, кто хранит информацию о них.[1116] Хартия также защищает лиц, которые в результате ошибочной информации были подвергнуты полицейским полномочиям (например, аресту или задержанию) или посягательствам на частную жизнь. Для оправдания посягательств на свободу или неприкосновенность частной жизни государство должно доказать наличие разумных оснований для оправдания такого вмешательства. Разумные основания для оправдания вмешательства в частную жизнь или свободу требуют индивидуальной оценки, что также защищает лиц, подвергшихся действию полиции (например, арест или задержание) или посягательств на частную жизнь в результате предоставления ошибочной информации. Чтобы оправдать вмешательство в свободу или личную жизнь, государство должно доказать, что имелись разумные основания для оправдания вмешательства. Стандарт разумных оснований для оправдания вмешательства в частную жизнь или свободу требует индивидуальной оценки[1117] и расследования того, является ли какая-либо информация, на которую полагаются с целью оправдания вмешательства, достаточно надежной и достоверной. Примечательно, что даже помимо проблем с неточностью данных, маловероятно, что стандарт разумных оснований может быть когда-либо удовлетворён на основе одних только алгоритмических прогнозов. [1118] По своей природе прогностические алгоритмы

[1115] Freedom of Information and Protection of Privacy Act, RSO 1990, c F.31, s 40(3); Municipal Freedom of Information and Protection of Privacy Act, RSO 1990, c M.56, s 30(3).

[1116] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29> at para 13. For example, given «people generally have little idea how, why, and for what reasons their information is collected, processed, and disclosed to other parties by the companies they entrust with their data", a web application called Access My Info (AMI) was designed by Open Effect and the Citizen Lab to help individuals to create justified requests for copies of their personal information from service providers: https://accessmyinfo.ca/#/.

[1117] R v Chehil, 2013 SCC 49 at para 40-43; R v Kang-Brown, [2008] 1 SCR 456. This problem is discussed further below in Section 5.5.1 («Algorithmic Policing and Generalized Suspicion").

[1118] «[T]the suspicion held by the police cannot be so broad that it descends to the level of generalized suspicion, which was described by Bastarache J., at para. 151 of A.M., as suspicion 'that attaches to a particular activity or location rather than to a specific person'." R v Chehil, 2013 SCC 49 at para 28.

вытесняют индивидуально оцениваемые характеризующиеся широтой статистические обобщения. [1119]

Опора на неточную информацию в технологиях алгоритмического контроля представляет дополнительную конституционную опасность. «Арест на основании источника, достоверность которого, в конце концов, неизвестна, нельзя назвать объективно обоснованным».[1120]Примечательно, что в контексте дел CPIC, в прецедентном праве существует противоречивое отношение к лицам, которые были арестованы на основании ошибки в базе данных CPIC. В некоторых случаях суды отказывались признать, что какое-либо нарушение имело место в результате ошибочной информации, если офицер, проверявший данные CPIC, считал, что они действительны на момент ареста.[1121]Анализ прецедентного права базы данных CPIC подчеркивает некоторые проблемы, которые возникают, когда правоохранительные органы стремятся использовать алгоритмические полицейские технологии, которые полагаются на существующие базы данных полиции, которые являются устаревшими или неточными. Это пример того, что иногда называют проблемой «мусор на входе, мусор на выходе». Если наборы полицейских данных подвержены ошибкам и вводятся в алгоритмические полицейские технологии, последующие прогнозы, предоставляемые этими алгоритмами (т.е. прогнозы преступной деятельности с помощью инструментов алгоритмической полиции, ориентированных на человека или местоположение), будут испорчены этими ошибками. Если правоохранительные органы будут полагаться на ошибочные алгоритмические прогнозы, это приведёт к неоправданному вмешательству в охраняемые Хартией интересы, такие как конфиденциальность или свобода, если правоохранительные органы будут действовать на основе этих алгоритмических прогнозов. Хотя маловероятно, что суды поспешат предположить, что использование новых технологий объективно разумно в отсутствие независимых доказательств, подтверждающих надёжность таких инструментов, случаи ошибок, связанных с CPIC, также демонстрируют уязвимость, с которой люди могут пострадать от неточных данных. Значимый доступ к средствам исправления ошибок может быть труднодостижимым. Учитывая, что личная информация, полученная в результате обработки данных, также защищена законодательством о конфиденциальности, применимые обязательства по точности актуальны не только для входных данных, содержащих личную информацию, но также и для алгоритмических выходных

[1119] Смотрите, например, "Как объясняет профессор Фредерик Шауэр, лица, принимающие решения, которые полагаются на статистически обоснованные, но не универсальные обобщения," одновременно рациональны и несправедливы ", потому что некоторые люди" актуарно оседланы "статистически обоснованными выводами, которые, тем не менее, неточны". Solon Barocas & Andrew D Selbst, «Big Data's Disparate Impact" (2016) 104 California Law Review 671 at 688.

[1120] See R v White, 2006 ONCJ 147 at para 27.

[1121] R v Clark, [2003] OJ No 1323 (CJ); R v Wilson, [2003] OJ No 4465 (Sup Ct).

данных. В Верховном суде Канады было установлено, что Исправительная служба Канады (CSC) не выполнила свое обязательство «принять все разумные меры для обеспечения того, чтобы любая информация о преступнике, которую она использует, была как можно более точной, актуальной и полной», полагаясь на определённые инструменты оценки рисков, чтобы сделать выводы о г-не Эверте.[1122] CSC использовал эти инструменты, несмотря на давнюю осведомленность о том, что инструменты, возможно, демонстрируют культурную предвзятость и что их применимость к правонарушителям из числа коренного населения, одним из которых был г-н Эверт, серьезно сомнительна.[1123]

Использование алгоритмов для анализа информации в социальных сетях на предмет рисков будущей преступной деятельности вызывает аналогичные опасения в отношении культурного контекста.[1124]Изучив программу Hub в Саскачеване, комиссар Саскачевана по информации и конфиденциальности пришел к выводу, что данные социальных сетей не должны подлежать сбору с помощью алгоритмической технологии государственными органами или служить основой для определения риска, поскольку социальные сети являются источником неточной информации.[1125] Использование автоматизированных инструментов затруднено при анализе языка, который сильно зависит от контекста и культурно-специфических особенностей, что не может быть адекватно отражено в наборах данных, используемых для обучения алгоритмов.[1126]Например, профессор Эндрю Фергюсон отмечает, что ключевые слова, относящиеся к бандам и перестрелкам («удар», «бег», «забастовка»,

---

[1122] Эверт против Канады, 2018 SCC 30 at 3. В этом случае обязательство по обеспечению точности данных вытекает из раздела 24 (1) Закона об исправительных учреждениях и условном освобождении (SC 1992, c 20), который в значительной степени напоминает раздел 6 (2) федерального Закона о неприкосновенности частной жизни: "Государственное учреждение принимает все разумные меры для обеспечения того, чтобы личная информация, используемая учреждением в административных целях, была как можно более точной, актуальной и полной". Privacy Act, RSC, 1985, c P-21, s 6(2).

[1123] Ewert v Canada, 2018 SCC 30.

[1124] Например, учитывая, что "люди, как правило, имеют мало представления о том, как, почему и по каким причинам их информация собирается, обрабатывается и раскрывается другим сторонам компаниями, которым они доверяют свои данные", веб-приложение под названием Access My Info (AMI) был разработан Open Effect и Citizen Lab для оказания помощи лицам в создании обоснованных запросов на копии их личной информации от поставщиков услуг: Jordan Pearson, «Researchers Claim AI Can Identify Gang Members on Twitter", Vice (1 November 2016), <https://www.vice.com/en_us/article/mg7kgx/researchers-claim-ai-can-identify-gang-members-on-twitter>.

[1125] Community Mobilization Prince Albert (Re), 2014 CanLII 81867 (SK IPC) at para 32-38.

[1126] См., например, Генеральная Ассамблея ООН, Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение, A/73/348 (29 августа 2018 года) <https://undocs.org/A/73/348 > в пункте 15. См. также широкий спектр исследований, демонстрирующих ненадежность ИИ для различения нюанса в области модерации контента на платформах социальных сетей, e.g., Natasha Duarte, Emma Llanso & Anna Loup, «Mixed Messages? The Limits of Automated Social Media Content Analysis" (November 2017), Center for Democracy & Technology <https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf>; Maarten Sap et al, «The Risk of Racial Bias in Hate Speech Detection" (Paper delivered at Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy, 28 July 2019) 1668; and Md Abul Bashar et al, «Misogynistic Tweet Detection: Modelling CNN with Small Datasets" in R Islam et al, eds, Data Mining: 16th Australasian Conference, AusDM 2018, Revised Selected Papers (Communications in Computer and Information Science, Volume 996).

«кепка» и «парк») также могут иметь отношение к бейсболу.[1127] Алгоритм, который не может различать два контекста, может привлечь внимание полиции к отдельным лицам на основе безобидных сообщений и подвергнуть этих лиц нарушениям конфиденциальности. Этот риск был признан представителем SPPAL, который заявил, что исследователи были осведомлены о риске, связанном с концепцией «мусор на входе - мусор на выходе» и новизной характера проводимых ими исследований. [1128]Однако, несмотря на осведомленность об этой проблеме, а также о выводах и рекомендациях уполномоченного по информации и конфиденциальности в отношении данных в социальных сетях, SPPAL, тем не менее, указала, что намеревается использовать источники данных с низкой точностью, такие как данные из социальных сетей.[1129]

Интересы государственной политики, цель эффективного правоприменения, а также нормы конфиденциальности и применимое законодательство - все это усиливает необходимость в соответствующих гарантиях, чтобы полицейские базы данных и алгоритмические методы обработки предоставляли правоохранительным органам точную и надежную информацию. Только на основе такой информации агентства должны принимать решения, которые повлияют на отдельных лиц, жертв и общественность в целом.

Разработка надёжных мер защиты конфиденциальности требует вложения ресурсов в надлежащее ведение полицейских баз данных, на которые полагаются (как уже требует полиция и прокуратура).[1130] Кроме того, правоохранительные органы должны интегрировать и полагаться на опыт технологов, которые могут предоставить объективные рекомендации по надёжности и точности методов обработки данных.

[1127] Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017), at 126.

[1128] Представитель SPPAL также отметил, что новый характер алгоритмических исследований политики в Канаде является еще одной причиной для обеспечения того, чтобы модели исследователей и разработчиков были максимально прозрачными: "Используются ли эти данные вообще правильно? Учитывая, что эта работа такая новая, нам не с чем ее сравнивать. Но если я опубликую что-то в журнале уголовного правосудия, кто-то может посмотреть на это и сказать: "Эй, CPIC отстает на два года" или "Вот некоторые вещи, которые вы не поймали для насильственных преступников." Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

[1129] Dr. Kiera Stockdale, Saskatoon Police Service, «Saskatchewan Police Predictive Analytics Lab Missing Persons Project: Year One", Defence Research and Development Canada (February 2019), <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc335/p809812_A1b.pdf>.

[1130] Brigitte Bureau, «RCMP database remains out of date, police and prosecutors say", CBC News (10 March 2015) <https://www.cbc.ca/news/

В фокусе внимания № 5

Технология распознавания лиц и нарушение прав на неприкосновенность частной жизни

Технологии алгоритмической политики могут представлять серьёзную угрозу праву на неприкосновенность частной жизни.[1131] Учитывая, что технология распознавания лиц является «инструментом, который может лишить «возможности анонимно ходить по улице»[1132], существует острая необходимость в общественном диалоге, регулировании, и чёткие ограничения относительно его потенциального использования. Технологии распознавания лиц могут позволить правоохранительным органам отслеживать и других людей, занимающихся своей повседневной деятельностью, и, как таковые, значительно усиливают интересы конфиденциальности в изображении лица.[1133]В результате применяется правовая защита в соответствии с правами человека и конституционным законодательством.[1134]Однако, как и в других случаях, технологии алгоритмического контроля, рассматриваемые в этом отчёте, инструменты распознавания лиц включают в себя сбор данных, обработку данных и методы обмена данными, которые еще не были в центре внимания судебной практики, из которых появятся подробные правила, которым должны следовать правоохранительные органы. Даже в отсутствие таких правил правоохранительные органы обязаны соблюдать права человека и конституционные меры защиты (например, те, которые применяются к биометрической информации, связанной с изображениями лиц), независимо от того, насколько хорошо эти права были конкретизированы в канадских судах. Регулирование посредством конкретных законов может решить существующую

[1131] See generally Clare Garvie, Alvaro Bedoya & Jonathan Frankle, «The Perpetual Line-Up: Unregulated Police Face Recognition in America" (18 October 2016) <https://www.perpetuallineup.org>.

[1132] Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It", The New York Times (18 January 2020), <https://www. nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

[1133] Комитет по правам человека Организации Объединенных Наций также признал в своем проекте замечания общего порядка № 37, что использование распознавания лиц и других технологий, позволяющих идентифицировать отдельных участников публичных собраний, может нарушать права на неприкосновенность частной жизни и должно подвергаться независимому контролю и надзору. UN Human Rights Committee, «Draft General Comment No. 37" (2019) <https://www.ohchr.org/EN/HRBodies/CCPR/ Pages/GCArticle21.aspx>, at para 69. Office of the Privacy Commissioner of Canada, «Metadata and Privacy: A Technical and Legal Overview" (October 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>;R v Spencer, [2014] 2 SCR 212; R v Rogers Communications, 2016 ONSC 70; R v Wise, [1992] 1 SCR 527. See also: R v Vu, [2013] 3 SCR 657; Riley v California, (2014) 573 US 373 (Supreme Court of the United States).

[1134] Research Group of the Office of the Privacy Commissioner of Canada, «Automated Facial Recognition in the Public and Private Sectors", Office of the Privacy Commissioner of Canada (March 2013), <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy- research/2013/fr_201303/#heading-005>; Office of the Information & Privacy Commissioner, «Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

неопределённость в этой области, установив чёткие и необходимые ограничения. Как указано в разделе 5.2.1 («Сбор данных: массовое наблюдение и общественное пространство»), правоохранительные органы должны получить предварительное судебное разрешение на использование электронных методов расследования, которые пытаются отслеживать или деанонимизировать лиц, которые участвуют в онлайн или публичной среде.[1135] Такие методы включают размещение устройств GPS-слежения на автомобилях или деанонимизацию действий человека в сети путем получения идентифицирующей информации абонента, связанной с определенным IP-адресом. Аргументы в пользу предоставления аналогичной защиты изображения лиц также убедительны.

Используя технологию распознавания лиц, правоохранительные органы потенциально могут отслеживать и деанонимизировать людей, которые свободно передвигаются в общественных местах и в Интернете, а пострадавшие не подозревают, что их изображения были собраны, обработаны или идентифицированы. Деанонимизация, в частности, происходит путём получения изображения неизвестного лица и последующего использования алгоритма для перекрёстной ссылки на изображение с другими базами данных для получения потенциального соответствия, которое приводит к идентификации. Нерегулируемое использование технологии распознавания лиц представляет как минимум три других проблемы для защиты интересов конфиденциальности в дополнение к подрыву анонимности в повседневной жизни.

Во-первых, практика сбора и хранения изображений правоохранительными органами не является областью, которая исторически была объектом целенаправленного регулирования и надзора. При рассмотрении последствий технологии распознавания лиц для конфиденциальности необходимо оценить два компонента систем: алгоритм обработки изображений и базу данных изображений. Создание баз данных изображений влечёт за собой разветвления конфиденциальности, поскольку оно включает сбор и хранение личной информации от отдельных лиц, а в связи с появлением новой технологии распознавания лиц ожидания конфиденциальности в изображениях лиц ослабляются. Системы распознавания лиц поднимают новые вопросы и вновь подчеркивают старые вопросы: кому должно быть разрешено устанавливать видеокамеры и для каких целей? Когда правоохранительные органы должны получить предварительное судебное разрешение перед сбором изображений, например, от частных компаний и онлайн-платформ? Уместны ли и достаточны ли существующие методы сохранения изображений, которые ранее были собраны правоохранительными органами?

[1135] R v Spenser? (2014) 2 SCR 212; R v Wise, [1992] 1 SCR 527.

Базы данных полицейских фотографий могут помочь решить вышеупомянутые вопросы. Фотографии, снятые полицией, получаются в результате проведения полицейских арестов[1136], а правоохранительные органы даже имеют право применять силу, если это необходимо для получения фотографии;[1137] это не процесс, основанный на согласии. Многие правоохранительные органы Канады сообщают об использовании (или планируют использовать) технологию распознавания лиц в своих базах данных о фотографиях[1138]. Однако базы данных с фотографиями могут содержать фотографии лиц, которым никогда не было предъявлено обвинение в уголовном преступлении, и которые были обвинения сняты или признаны невиновными. Физические лица имеют конституционно защищенное право на неприкосновенность частной жизни в отношении их отпечатков пальцев и изображений, сделанных с помощью кружков.[1139] В частности, несанкционированное сохранение изображений является неконституционным.[1140] На практике, однако, каждая полицейская служба имеет свою собственную внутреннюю политику в отношении уничтожения биометрических данных, и эта политика обычно влечёт за собой дискреционный, основанный на запросе или даже платный процесс.[1141]

Во-вторых, технология распознавания лиц ненадёжна, особенно в случае расовых людей и женщин, которые с большей вероятностью будут ошибочно идентифицированы технологией.[1142] Деанонимизация, в частности, происходит путём взятия изображения неизвестного лица и последующего использования алгоритма для перекрёстной привязки изображения с другими базами данных изображений для получения потенциального совпадения, которое приводит к идентификации.

Нерегулируемое использование технологии распознавания лиц создаёт по крайней мере три другие проблемы для защиты интересов конфиденциальности в дополнение к разрушению анонимности в повседневной жизни. Практика сбора и хранения изображений правоохранительными органами не является областью, которая исторически являлась объектом целенаправленного

[1136] Identification of Criminals Act, RSC, 1985, c I-1.
[1137] Identification of Criminals Act, RSC, 1985, c I-1, at s 2(2).
[1138] See Section 4.3.3 («Facial Recognition").
[1139] R v Dore, [2002] OJ No 2845 (CA).
[1140] R v Strickland, 2017 BCPC 1, and 2017 BCPC 211; R v Dore, [2002] OJ No 2845 at paras 64-71 (CA).
[1141] See for example Lin v Toronto Police Services Board, [2004] OJ No 170 (SCJ); Information and Privacy Commissioner of Ontario, Privacy Complaint No. MC-060020-1 (21 December 2007), <https://decisions.ipc.on.ca/ipc-cipvp/privacy/en/135086/1/document.do>.
[1142] Danielle Groen, «How We Made AI as Racist and Sexist as Humans", The Walrus (12 November 2019), <https://thewalrus.ca/how-we-made- ai-as-racist-and-sexist-as-humans/>; Drew Harwell, «Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use", The Washington Post (19 December 2019), <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms- racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>; and Russell Bramdon, «Amazon's facial recognition matched 28 members of Congress to criminal mugshots", The Verge (26 July 2018), <https://www.theverge.com/2018/7/26/17615634/amazon-rekognition- aclu-mug-shot-congress-facial-recognition>.

регулирования и надзора. При рассмотрении последствий технологии распознавания лиц для конфиденциальности необходимо оценить два компонента системы: алгоритм, который обрабатывает что выбрано, или что обработано или идентифицировано. Деанонимизация, в частности, происходит путём получения изображения неизвестного лица и затем с помощью алгоритма перекрёстной ссылки на изображение с другими базами данных обработанных изображений.

Алгоритмы распознавания лиц сопоставляют совпадения по вероятности. Один поиск может генерировать несколько ранжированных совпадений.[1143]Однако, исследователи и правительственные исследования сообщают, что системы распознавания лиц различаются по степени точности. Например, исследователи из Соединенных Штатов определили, что коммерческое программное обеспечение для распознавания лиц даёт ошибки при идентификации темнокожих женщин более чем в одной трети случаев и только в 0,8 процента случаев у белых мужчин.[1144] Кроме того, в отчёте Big Brother Watch за 2018 год указали, что NeoFace Watch, продукт для распознавания лиц от NEC Corporation – компании, у которой CPS и TPS приобрели свои технологии распознавания лиц, – в 91-98% случаев выдаёт неточные совпадения, используемые столичной полицией и полицией Южного Уэльса в Соединенном Королевстве.[1145] В июне 2020 года начальник полиции Детройта Джеймс Крейг признал, что технология распознавания лиц, используемая полицией Детройта, разработанная DataWorks Plus, в 96% случаев неверно идентифицирует людей.[1146]Такие результаты вызывают вопросы о надёжности техники, которая может привести к аресту или привлечению к уголовной ответственности на основании неправильной идентификации.

Распознавание лиц: я могу разблокировать телефон сестры, и мы не близнецы. – Центр судебных исков чернокожего населения (Black Legal Action Center (BLAC).[1147]

Третье, растущие уровни сбора изображений и обмена ими между частным сектором и правоохранительными органами требуют агрессивных действий для обеспечения прозрачности, надзора и чётких ограничений на использование. В январе 2020 года New York Times сообщила, что компания Clearview AI участвовала в массовой агрегации общедоступных и

[1143] Ian Sample, «What is facial recognition - and how sinister is it?", The Guardian (29 July 2019), <https://www.theguardian.com/ technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it>.

[1146] Jason Koebler, «Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time", VICE Motherboard (29 June 2020), < https:// www.vice.com/en_ca/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time>.

[1147] Interview of Black Legal Action Center by Cynthia Khoo (12 july 2019).

полуобщественных изображений, сканируя Интернет, и использовала эти изображения для разработки технологии распознавания лиц, которую компания затем предоставила в качестве продукта для правоохранительных органов.[1148]Clearview AI позже выяснил, что у неё были контракты с канадскими правоохранительными органами, но не раскрыл, какие именно. Это произошло только после утечки внутренней информации.

После этого в новостях стало известно, что канадские правоохранительные органы сами предоставили минимальную информацию о том, использовали ли их соответствующие полицейские службы продукт компании для распознавания лиц.

Такая информация, как тот факт, что канадские полицейские службы тестируют противоречивую технологию распознавания лиц, не должна быть доступной для общественности только после публикации в средствах массовой информации, демонстрируя необходимость активной прозрачности и практики надзора. Тот факт, что Clearview AI позже приостановил свой контракт с RCMP и объявил о прекращении операций в Канаде, не устраняет этот дефицит демократии.[1149] Предыдущие попытки определить, какие агентства использовали технологию Clearview AI, были заблокированы: журналисты получали неверную информацию. от агентств; компания отказалась объяснить законность сбора или предоставления информации канадским агентствам; и канадская общественность и политики были (по крайней мере временно) не в состоянии оценить, какие меры контроля или ограничения применялись или должны быть применены к технологии, и всё из-за катастрофической неспособности агентств обеспечить прозрачность своей деятельности. Такие случаи, как Clearview AI, подчёркивают критическую потребность в государственных процессах, связанных с технологиями алгоритмического контроля, чтобы значимо гарантировать достаточную прозрачность, надзор и чёткие ограничения на принятие и использование этих технологий – вплоть до превентивных запретов, учитывая очевидную опасность лица технология распознавания в частности. Кроме того, перечень запретов и мораторий, которые муниципалитеты и промышленные предприятия уже ввели в Соединенных Штатах, как описано в разделе 4.3.3 («Распознавание лиц») настоящего отчёта, является дополнительным свидетельством фундаментальной угрозы, которую представляет технология распознавания лицк праву на неприкосновенность частной жизни и другим правам и свободам

[1148] Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It", The New York Times (18 January 2020), <https://www. nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; «Privacy watchdogs to probe Clearview AI's facial-recognition technology", CBC News (21 February 2020), <https://www.cbc.ca/news/canada/toronto/clearview-ai-police-use-1.5471493>.

[1149] Thomas Daigle, «Clearview AI stops offering facial recognition software in Canada amid privacy probe," CBC (6 July 2020) <https://www. cbc.ca/news/technology/clearview-ai-stops-facial-recognition-in-canada-1.5639380

человека, особенно к тем исторически маргинализированным группам, которые непропорционально подвергаются наблюдению со стороны полиции.

5.2.5. Заключительные комментарии: алгоритм действий и право на конфиденциальность

Инструменты алгоритмического контроля, такие как алгоритмическое наблюдение и прогнозы, ориентированные на человека, реализуют право на неприкосновенность частной жизни в результате методов сбора, обработки и обмена данными, на которые по своей природе склонны полагаться алгоритмические инструменты. Права человека и конституционная юриспруденция, относящиеся к защите частной жизни, содержат рекомендации о том, как интересы конфиденциальности могут быть задействованы при использовании такой новой технологии. Судебная практика признает необходимость защиты конфиденциальности в отношении личной информации, которая доступна в публичных местах. В то время как раздел 8 юриспруденции в Канаде имеет тенденцию относиться к методам сбора данных правоохранительными органами, раздел 8 и законодательство о конфиденциальности также применяются к методам обработки и обмена данными, которые явно затрагивают интересы конфиденциальности.

Поскольку правоохранительные органы стремятся получить доступ к новым классам или беспрецедентным объёмам данных об отдельных лицах и сообществах, часто при использовании продуктов, предоставляемых частными компаниями, правовые гарантии и конституционные меры защиты должны идти в ногу с тем, чтобы защищать права всех людей. В частности, эти меры безопасности должны гарантировать, что отдельные лица не будут подвергаться необоснованному вмешательству в охраняемые интересы конфиденциальности со стороны правоохранительных органов, а также гарантировать, что защищенные зоны конфиденциальности не будут подорваны расширением полицейских методов сбора данных и возможностей наблюдения.[1150] Использование технологий алгоритмического контроля,

[1150] Генеральная Ассамблея ООН, Совет ООН по правам человека и Верховный комиссар ООН по правам человека признали опасность массового наблюдения и необходимость пересмотра права на неприкосновенность частной жизни в свете современных проблем, возникающих в связи с технологическим прогрессом. See UN General Assembly, «Resolution adopted by the General Assembly on 18 December 2013: 68/167, The right to privacy in the digital age", (21 January 2014) <https://undocs.org/A/RES/68/167>; UN Human Rights Committee, «Resolution adopted by the Human Rights Council on 23 March 2017: 34/7, The right to privacy in the digital age", (7 April 2017) <https://undocs.org/A/HRC/RES/34/7>; UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, and UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29> at para 17.

которые могут нарушать конфиденциальность, должно быть ограничено необходимым и соразмерным использованием, чтобы защитить зону конфиденциальности в общественной жизни, на которую люди имеют право рассчитывать, чтобы они могли пользоваться основными свободами, такими как свобода выражения. Обеспечение безопасности такой зоны должно включать механизмы судебного надзора за формами обработки данных и совместного использования данных, которые создают новые проблемы конфиденциальности, которые не решаются должным образом в рамках существующего в Канаде ордера на обыск и режима производственного порядка.

Право на свободу выражения мнений, мирных собраний и объединений

Права на свободу выражения мнений, мирных собраний и ассоциаций защищены статьями 19, 21 и 22 ICCPR.[1151]и разделом 2 Хартии.[1152] Эти свободы имеют основополагающее значение для демократического общества и для поощрения и защиты широкого круга других прав человека.[1153]

Права на мирные собрания и свободу объединений особенно ценны, поскольку они позволяют маргинализованным лицам объединяться, чтобы исправить дисбаланс сил и защитить себя от более могущественных образований.[1154]Технологии алгоритмической полицейской деятельности рискуют затруднить осуществление основных свобод выражения мнений, мирных собраний и ассоциаций. Растущий объём эмпирических данных показывает связь между государственным онлайн-наблюдением, включая простую перспективу такого наблюдения, и сдерживающим воздействием на свободу выражения мнения.[1155] Существенные сдерживающие эффекты, которые могут быть вызваны государственным наблюдением, включают в себя

[1151] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, arts 19, 21, 22.

[1152] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, s 2.

[1153] UNHRC, General Comment No 34 on Article 19 (Freedoms of opinion and expression), 102nd Sess, adopted 12 September 2011, UN Doc CCPR/C/GC/34, at paras 2-3 <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>; UNHRC, General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 1-2 <https://www.ohchr.org/EN/HRBodies/CCPR/ Pages/GCArticle21.aspx>; Mounted Police Association of Ontario v. Canada (Attorney General), 2015 SCC 1 at para 48.

[1154] UNHRC, General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 2 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>; Mounted Police Association of Ontario v. Canada (Attorney General), 2015 SCC 1 at para 58.

[1155] See Jonathon W Penney, «Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 Internet Policy Review 22; Alex Marthews and Catherine E Tucker, «The Impact of Online Surveillance on Behavior" in David Gray and Stephen E Henderson, eds, The Cambridge Handbook of Surveillance Law (Cambridge, Cambridge University Press, 2017), at 437; and Margot E Kaminski and Shane Witnov, «The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech" (1 January 2015) 49 University of Richmond Law Review.

то, что люди с меньшей вероятностью будут участвовать в определённых законных действиях или с большей вероятностью будут проявлять большую осторожность, когда они участвуют в такой деятельности, в том числе в отношении онлайн-речи, онлайн-поиска и обмена лично созданными контентами в социальных сетях.[1156]В этом разделе отчета обсуждаются, в частности, два вопроса, связанные с негативным воздействием алгоритмических полицейских технологий на права на свободу выражения мнений, мирных собраний и ассоциаций. В разделе 5.3.1 анализируется, как технологии алгоритмического контроля могут подорвать анонимность толпы на публичных собраниях, что представляет собой беспрецедентный уровень технологического вторжения в фундаментальные свободы, которые защищает такая анонимность.

В разделе 5.3.2 описывается исследование о том, каким образом алгоритмические полицейские технологии влияют на маргинализированные сообщества, обеспечивая алгоритмическое наблюдение за протестной активностью и социальными движениями. Такой вид целевого мониторинга вызывает особые опасения в отношении прав человека и Хартии, учитывая исторический контекст непропорционального надзора со стороны правоохранительных органов за маргинализованными сообществами и защитниками прав человека. Важность защиты этих основных свобод подчёркивается с учётом их взаимосвязи с другими правами человека, такими как права на равенство и неприкосновенность частной жизни.

5.3.1. Подрыв анонимности толпы на публичных собраниях

Развёртывание правоохранительными органами новых и быстро развивающихся технологий наблюдения, таких как распознавание лиц и автоматическое считывание номерных знаков, ставит под угрозу анонимность, которая служила условием для осуществления основных свобод выражения мнений, мирных собраний и ассоциаций.

Исторически сложилось так, что участники массовых демонстраций могли полагаться на относительную анонимность толпы, чтобы защитить свою личность от работодателей, правоохранительных органов или других властей; анонимность позволяет более полно пользоваться основными свободами при снижении риска репрессий.[1157]Однако, технология распознавания лиц

[1156] Jonathon W Penney, «Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017) 6:2 Internet Policy Review 22.

[1157] Privacy International, «Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR", <https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf>; UNHRC,

потенциально может идентифицировать этих людей по изображениям или видео, снятым на публичных собраниях, с гораздо большей лёгкостью, чем попытки правоохранительных органов идентифицировать людей без такой технологии. Таким образом, распознавание лиц и аналогичные возможности могут подорвать анонимность, которая облегчила участникам осуществление их основных свобод. Правоохранительные органы начали применять эту технологию на протестующих. В Соединенном Королевстве полицию Южного Уэльса обвинили в использовании системы распознавания лиц во время мирной акции протеста против оружия.[1158] В Канаде полицейские в Торонто и Калгари могут отправлять изображения людей, снятые на публичных собраниях, в свои собственные программы распознавания лиц для поиска совпадений с их соответствующими базами данных фотографий.[1159]Эти формы алгоритмического наблюдения подчеркивают взаимосвязь между защитой конфиденциальности как анонимности и другими основными свободами, такими как свобода выражения мнений и свобода ассоциаций.[1160]Кроме того, лица, которые принимают меры, чтобы избежать идентификации системами распознавания лиц, могут рассматриваться как подозрительные и потенциально оштрафованные за их попытки сохранить свою анонимность. Такие штрафы назначены в Великобритании.[1161]В Канаде в 2012 году было принято уголовное наказание за ношение масок во время беспорядков и незаконных собраний (разделы 65 и 66 Уголовного кодекса). [1162]Критики опасаются, что этот запрет может сдержать или помешать мирной протестной деятельности.[1163] Общий комментарий Комитета ООН по правам человека о праве на мирные собрания гласит, что меры участников по защите своей анонимности не должны подлежать общему запрету.[1164]Таким образом, алгоритмические полицейские

General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 2 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21. aspx>.

[1158] Ed Bridges, «Why I'm Challenging Cardiff Police On Their Invasive Facial Recognition Technology", Huff Post Blog (14 June 2018) <https://www.huffingtonpost.co.uk/entry/facialrecognition_uk_5b227088e4b0bbb7a0e53760?guccounter=1>

[1159] Для получения дополнительной информации об использовании канадскими полицейскими службами технологии распознавания лиц см. раздел 4.3.3 ("Распознавание лиц") и IN FOCUS # 5: Технология распознавания лиц и размывание прав на конфиденциальность в разделе 5.2.4 ("Точность данных: неточные данные и неточные алгоритмы").

[1160] R v Wise, [1992] 1 SCR 527 at 558; R v Spencer, [2014] 2 SCR 212 at para 44.

[1161] Lizzie Dearden, «Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested", Independent (31 January 2009) <https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met- police-face-cover-man-fined-a8756936.html>.

[1162] Office of the Privacy Commissioner of Canada, «Automated Facial Recognition in the Public and Private Sectors" (March 2013) < https:// www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/#fn8-rf>; Criminal Code, RSC, 1985, c C-46, ss 65(1) and 66(1).

[1163] Office of the Privacy Commissioner of Canada, «Automated Facial Recognition in the Public and Private Sectors" (March 2013) <https:// www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/#fn8-rf>; «New Bill Refines Rules on Masks in Unlawful Protests", The Globe and Mail (1 November 2012) <https://www.theglobeandmail.com/news/politics/new-bill-refines-rules-on-masks-in- unlawful-protests/article4845550.

[1164]UNHRC, General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 60 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

технологии - особенно в сочетании с законами, исключающими законные попытки по предотвращению такой государственной слежки - могут иметь эффект значительного разрушения конфиденциальности в виде анонимности, в результате чего нарушаются права на свободу выражения мнений, мирных собраний и ассоциаций.

5.3.2. Наблюдение за социальными движениями и маргинализованными сообществами

Использование алгоритмических инструментов интеллектуального анализа данных в социальных сетях для мониторинга онлайн-разговоров на целевые темы или между ними увеличивает риск того, что люди будут участвовать в самоцензуре, если они знают или подозревают, что их речь контролируется государственными органами.[1165] Точно так же люди могут избегать свободного использования своей свободы на ассоциации, если полицейские алгоритмы используются для отслеживания социальных сетей и принадлежности к группам, например, через систему алгоритмического анализа социальных сетей CPS, или даже если люди только подозревают, что полиция может отслеживать такую информацию.[1166] Такое сдерживающее воздействие может особенно остро сказаться на маргинализированных сообществах. В эти общины входят те, кто подвергался непропорциональному надзору со стороны полицейских служб и других государственных органов или у кого есть основания не доверять канадским правоохранительным органам.

Технология используется против нас [черных], когда мы пытаемся отстаивать свои права. Мониторинг активистов действительно страшен. Это заставляет замолчать, потому что ты так напуган. – Центр судебных исков чернокожего населения (Black Legal Action Center (BLAC)). [1167]

Внимание канадских правоохранительных органов к протестам и демонстрациям приводит к особенно серьёзным негативным последствиям для маргинализированных сообществ, затрагивая их право на мирные собрания,[1168] в дополнение к их праву на свободу выражения мнения. Обсуждая «Project

---

[1165] Glenn Greenwald, «New Study Shows Mass Surveillance Breeds Meekness, Fear and Self-Censorship", The Intercept (28 April 2016) <https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/>.

[1166] See J. W. Penney, «Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 Internet Policy Review 22; A. Marthews and C. Tucker, «The Impact of Online Surveillance on Behavior" in D. Gray and S. E. Henderson, eds., The Cambridge Handbook of Surveillance Law (2017) 437; and Kaminski, Margot E. and Witnov, Shane, «The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech" (January 1, 2015). University of Richmond Law Review, Vol. 49, 2015.

[1167] Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

[1168] UNHRC, General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 2 and 36 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

Wide Awake»,[1169] RCMP специально упомянула свой «проактивный» анализ сообщений в социальных сетях, чтобы предсказать, может ли преступление произойти во время демонстрации, и оценить, есть ли необходимость в увеличении присутствия полиции на мирных протестах на этой основе.[1170]

Такая практика ставит под сомнение необходимость или соразмерность такого наблюдения, учитывая превентивность осуществляемого наблюдения и ненасильственный характер исследуемых событий.

Полицейская служба Оттавы также отслеживала активность протестующих в социальных сетях во время демонстраций.[1171] Мониторинг социальных движений, стремящихся к равенству, представляет особую опасность для групп, отстаивающих демократические права и свободы исторически неблагополучных или маргинализированных сообществ. Например, в 2016 году находящаяся в Онтарио компания Media Sonar подверглась критике за то, что рекламировала себя правоохранительным органам США как способ отслеживания хэштегов, связанных с социальными движениями, протестующими против жестокости полиции, включая #BlackLivesMatter.[1172]Полиция Калгари и Торонто в прошлом заключала контракты с Media Sonar; однако, похоже, они прекратили использование программного обеспечения.[1173] Сотрудник правоохранительных органов из Калгари предположил, что решение агентства прекратить его использование было связано с уменьшением полезности программного обеспечения после того, как программное обеспечение потеряло способность доступа к основным платформам социальных сетей,[1174] из чего следует, что это решение не представляло принципиального противодействия целенаправленной слежке за определёнными социальными движениями. Программное обеспечение потеряло доступ в результате того, что платформы социальных сетей, такие как Twitter и Instagram (дочерняя компания Facebook), запретили Media Sonar за нарушение их политики конфиденциальности и политики использования

[1169] Project Wide Awake was introduced in more detail under «Social Media Surveillance" in Section 4.3 («Algorithmic Surveillance Tools").

[1170] Bryan Carney, «'Project Wide Awake': How the RCMP Watches You on Social Media", The Tyee (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>.

[1171] Nathan Munn, «'Predictive Policing' Is Coming to Canada's Capital, and Privacy Advocates Are Worried", VICE Motherboard (13 February 2017) <https://www.vice.com/en_us/article/jpaew3/ottawa-police-strategic-operations-centre-canada-surveillance>.

[1172] ACLU Northern California, «This Surveillance Software is Probably Spying on #BlackLivesMatter" (15 December 2015) <https://www.aclunc. org/blog/surveillance-software-probably-spying-blacklivesmatter>. Обе полицейские службы, как представляется, прекратили использование программного обеспечения, при этом один из сотрудников правоохранительных органов Калгари предположил, что решение о прекращении его использования было обусловлено меньшей полезностью программного обеспечения после того, как ему был запрещен доступ к основным платформам социальных сетей.

[1173] See Toronto Police Services Board, «Public Meeting - Agenda, April 20 2017", <http://www.tpsb.ca/images/agenda_apr20_public_main. pdf>, at p 5; Email from CPS FOI office to YS, 19 December 2018.

[1174] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

платформы соответственно.[1175]Полицейская служба Торонто, как сообщается, также отслеживала активность в социальных сетях, связанную с движением Black Lives Matter, используя методы, которые на момент написания статьи не были публично раскрыты.[1176] Законы об уголовном правосудии, полицейская практика и деятельность по наблюдению должны быть изучены в контексте продолжающегося наследия дискриминационного наблюдения канадскими правоохранительными органами за отдельными лицами и общественными движениями, имеющими отношение к правам коренных народов, расовой справедливости и другой защите прав человека.[1177]

Учитывая важность протеста и демократического инакомыслия для осуществления основных свобод, надзор со стороны правоохранительных органов должен подвергаться тщательной проверке, особенно в тех случаях, когда контролируемые лица выступают с позиций исторического бесправия или угнетения. Журналист, писатель и активист Десмонд Коул заявил: «Одна из наиболее важных характеристик слежки - это то, как она меняет наше поведение как целей. Это буквально меняет наш разум. Это заставляет задуматься о том, что за нами наблюдают. Даже если нет. Это подталкивает нас к саморегулированию, и мы должны этому противостоять. Что касается меня, я стал гораздо больше осознавать идею, что за мной наблюдают; я думаю, было бы невозможно не допустить, чтобы это каким-либо образом повлияло на меня

[1175] Andrew Margison, «Twitter and Instagram ban London, Ont., company for helping police track protesters", CBC News (19 January 2017) <https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093>.

[1176] Stephen Davis, «Police monitored Black Lives Matter Toronto protesters in 2016, documents show", CBC News (3 May 2018) <https://www. cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628>.

[1177] См., например, комментарии Джонатана Рудина, представленные в "IN FOCUS # 1: Community Perspectives on Algorithmic Policing", в Части 2 ("Социальный и исторический контекст"). Интервью Джонатана Рудина Синтии Хоо и Йоланды Сонг (8 мая 2019). В последнее время эти тенденции нашли свое отражение в наблюдении полиции за движением "Не надо больше" и другими демонстрациями коренных народов: Jorge Barrera, «Aboriginal Affairs shared wide range of information with spy agency to bolster Idle No More surveillance: documents", National News (18 March 2015). <https://aptnnews.ca/2015/03/18/ aboriginal-affairs-shared-wide-range-information-spy-agency-bolster-idle-surveillance-documents/>; Hillary Beaumont, «Canadian police spied on Indigenous protesters on Parliament Hill", VICE (10 November 2017) <https://news.vice.com/en_ca/article/a3jjxa/canadian-police-spied-on- indigenous-protesters-on-parliament-hill>; Hillary Beaumont, «Canada's spy agency has been watching Standing Rock and thinks it has Canadian implications", VICE (15 March 2017) <https://news.vice.com/en_ca/article/evaw3w/canadas-spy-agency-has-been-watching-standing-rock-and- thinks-it-has-canadian-implications>. In 2014, the RCMP established Project SITKA to collect information about prominent Indigenous activists and assess their levels of «threat" (assessed as a likelihood that the individual has committed or will likely commit criminal activity): Sean Craig, «RCMP tracked 89 indigenous activists considered 'threats' for participating in protests", The National Post (13 November 2016) <https:// nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests>. Исследователи Майлз Хоу и Джеффри Монахан обнаружили, что расследование КККП выходило далеко за рамки преступной деятельности и охватывало не только протесты, но и выступления в турах и другие события, "жалобы аборигенов могут быть частью темы": Miles Howe & Jeffrey Monaghan, «Strategic Incapacitation of Indigenous Dissent: Crowd Theories, Risk Management, and Settler Colonial Policing" (2018) 40:4 Canadian Journal of Sociology at 334. The researchers found «the RCMP's understanding of risk [or threat] to be synonymous with the potential of a protest movement's success ... suggest[ing] that the RCMP's mandate has warped toward working to undermine protest movements, regardless of their legality": Miles Howe & Jeffrey Monaghan, «Policing Indigenous Dissent: Trends Behind Wet'suwet'en Raid" (28 January 2015) 5 Culturally Modified <https:// culturallymodified.org/policing-indigenous-dissent-trends-behind-the-wetsuweten-raid/>.

и то, как я работаю, но я стараюсь осознавать это. Я активно стараюсь не бояться и не заставлять себя молчать.»[1178]'Непропорциональное нацеливание на методы наблюдения со стороны правоохранительных органов поднимает фундаментальные вопросы о дискриминации. Ограничения права на мирные собрания должны быть «нейтральными по содержанию» и не основываться на расе, этнической принадлежности, политических взглядах, сексуальной ориентации или других защищаемых или смежных факторах; любые ограничения также должны быть необходимыми и соразмерными в контексте защиты демократии и прав человека. [1179] Лица, которые участвуют в социальных движениях, которые с большей вероятностью будут контролироваться правоохранительными органами, такими как движения за права коренных народов или движения за расовую справедливость, вероятно, лишены равной защиты закона в соответствии с ICCPR. Эти же группы могут быть несправедливо чрезмерно представлены в наборах полицейских данных, которые в конечном итоге могут быть использованы для обучения полицейских алгоритмов, тем самым заставляя правоохранительные органы направлять дополнительное непропорциональное внимание и ресурсы полиции на эти конкретные группы и сообщества.

Толкуя Хартию, Верховный суд Канады ясно дал понять, что права человека и основные свободы, закрепленные в Хартии, следует толковать как единую систему, которая поддерживает свои основные ценности и внутренне согласована во всем.[1180] Таким образом, любое исследование воздействия полицейской практики, которая систематически отслеживает онлайн-активность, протесты и формы активности посредством алгоритмического агрегирования и анализа данных, требует рассмотрения глобального воздействия этой практики на права и свободы человека, которые связаны с неприкосновенностью частной жизни, выражения мнений, ассоциаций и равенством вместе. Защита частной жизни в соответствии с разделом 8 Хартии, например, была описана как «предвестник» осуществления других прав и основных свобод, охраняемых Хартией. Таким образом, любое исследование воздействия полицейской практики, которая систематически отслеживает онлайн-активность, протесты и формы активности посредством алгоритмического агрегирования и анализа данных, требует глобального рассмотрения воздействия этой практики на права и свободы человека, которые связаны с неприкосновенностью частной жизни, выражением мнений, объединением и равенством вместе. Защита частной жизни в соответствии с разделом 8 Хартии, например, была описана как «предвестник» осуществления

[1178] Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).
[1179] UNHRC, General Comment No 37 on Article 21 (Right of peaceful assembly), 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 22 and 40 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.
[1180] R v S (RJ), [1995] 1 SCR 451 at 561; Health Services and Support - Facilities Subsector Bargaining Assn v British Columbia, [2007] 2 SCR 391 at paras 80-86.

других прав и основных свобод, защищённых Хартией, вместе взятых. Защита частной жизни в соответствии с разделом 8 Хартии, например, была описана как «предвестник» осуществления других прав и основных свобод, охраняемых Хартией, таких как свобода выражения мнения.[1181]

Верховный суд Канады признал эту неотъемлемую связь между конфиденциальностью (например, анонимностью в публичном пространстве) и свободой выражения. Возможность свободного передвижения без постоянного надзора со стороны правительства – важный источник личной свободы, который должен быть решён. Боязнь систематического наблюдения даже в общественных местах разрушает это чувство свободы. Судья Дуглас признал важность этой ценности конфиденциальности в демократическом обществе, комментируя, что свободное передвижение так же опасно для тирана, как свободное выражение идей или право на собрания, и, следовательно, контролируется в большинстве стран.[1182]

Учитывая важность поставленных на карту прав, влиянию технологий алгоритмического контроля над основными свободами следует уделять должное внимание даже там, где есть законные цели правоохранительных органов. Такое взвешивание должно включать признание того, что люди обычно не ожидают, что их действия в Интернете будут систематически и интенсивно отслеживаться и анализироваться правоохранительными органами, и не следует ожидать, что люди будут вести свою жизнь под бременем такого предположения. В результате там, где задействованы такие права, важна тщательная проверка алгоритмических методов полицейской деятельности для проверки их соразмерности, законности и необходимости с точки зрения общественных интересов цели.[1183]

[1181] Renee Pomerance, «Informational Privacy in the Digital Age," in Benjamin Berger, Emma Cunliffe, and James Stribopoulos, eds, To Ensure that Justice is Done: Essays in Memory of Marc Rosenberg (Toronto: Thomson Reuters, 2017), at p 183.

[1182] R v Wise, [1992] 1 SCR 527 at 558 per La Forest J., which was endorsed by the unanimous court in R v Spencer, [2014] 2 SCR 212 at para 44.

[1183] UN General Assembly, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, A/74/349 (11 September 2019) <https://undocs.org/A/74/349> at para 61.

5.3.3. Заключительные комментарии: алгоритмическая деятельность полиции и право на свободу выражения мнения, мирных собраний и ассоциаций

Изучив проблемы, которые возникают при алгоритмической полицейской деятельности в контексте прав на свободу выражения мнений, мирных собраний и ассоциаций, становится очевидным, что использование алгоритмических полицейских технологий чревато ограничением реализации этих основных свобод.[1184] Инструменты наблюдения, такие как технология распознавания лиц, угрожают анонимности толпы, которая традиционно защищала личности протестующих. Растущий объём эмпирических данных показывает, что использование программного обеспечения для наблюдения за социальными сетями для отслеживания общения и действий протестующих также может оказывать сдерживающее воздействие на защищаемые свободы. Мониторинг протестной активности и общественных движений вызывает озабоченность в историческом контексте непропорционального надзора со стороны правоохранительных органов против расового правосудия и защитников прав коренных народов. Расовые и маргинализованные общины могут особенно остро пострадать от негативного воздействия. Защита основных свобод важна в этом контексте для обеспечения того, чтобы исторически обездоленные или маргинализированные общины имели в равной степени значимый доступ к свободе организации и участия в общественной жизни.

Право на равенство и свободу от дискриминации

Канадская система уголовного правосудия и правоприменительная практика неоднократно подвергались критике со стороны различных органов и экспертов ООН за их дискриминационное воздействие на маргинализированные группы, такие как коренное и расовое население.[1185] Это

[1184] R v Khawaja, 2012 SCC 69 at paras 79-80; Canadian Broadcasting Corporation v Attorney General of Ontario, 2015 ONSC 3131 at para 168.

[1185] В 2004 году Специальный докладчик ООН по современным формам расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости выразил крайнюю обеспокоенность по поводу высокого уровня лишения свободы коренных, черных и азиатских лиц в Канаде: доклад Специального докладчика г-на Дуду Дьена о современных формах расизма, расовой дискриминации, ксенофобии и связанной с ними нетерпимости; Комитет по ликвидации расовой дискриминации также отметил чрезмерную представленность африканских канадцев в системе уголовного правосудия и непропорционально высокую степень, с которой полицейские допросы и сбор данных затрагивают лиц африканского происхождения: Комитет Организации Объединенных Наций по ликвидации расовой дискриминации, Краткий отчет 2600-е заседание, CERD / C / SR.2600, п. 34; и Независимый эксперт УВКБ ООН по вопросам меньшинств также написал: «Лица, принадлежащие к африканским канадским, мусульманским, арабским и латиноамериканским общинам, сообщали о том,

негативное и непропорциональное воздействие также распространяется на бездомных, страдающих психическими заболеваниями или принадлежащих к ЛГБТ-сообществу, включая тех, кто существует на пересечении нескольких причин уязвимости или притеснения. [1186]Хотя правительство Канады предприняло определенные усилия по предотвращению дискриминации в уголовном правосудии, [1187] члены исторически маргинализованных сообществ в подавляющем большинстве несут на себе основную тяжесть нарушений прав человека и несоразмерных преследований со стороны правоохранительных органов.[1188] Такая дискриминация усугубляется тем, что технологии алгоритмического полицейского контроля могут опираться на предвзятые и неточные данные, которые в настоящее время хранятся или на которые полагаются правоохранительные органы, например, данные с остановок полиции, базы данных банд, публичные отчёты, аресты, признания вины и неправомерные приговоры.[1189] Эти технологии рискуют увековечить или усилить существующее неравенство таким образом, чтобы это равносильно нарушению права на равенство и права на свободу от дискриминации маргинализованных групп, которые защищены разделом 15 Хартии прав и свобод Китая («Хартия»).[1190] В разделе 5.4 широко анализируется, как алгоритмические методы работы полиции поднимают вопросы, затрагивающие право на равенство и право на свободу от дискриминации. В разделе 5.4.1 описывается объём права на равенство и свободу от дискриминации в канадском и международном праве прав человека. В разделе 5.4.2 исследуется алгоритмическая предвзятость и то, как технология алгоритмического контроля может привести к «петлям обратной связи несправедливости»[1191] которые могут подвергнуть маргинализированные сообщества повышенному подозрению и более высокому риску того, что правоохранительные органы будут применять силу или чрезмерную силу. Такие петли обратной связи также могут ухудшить автономию, благополучие и достоинство сообщества.

В разделе 5.4.3 анализируется, как основанная на данных природа алгоритмической полицейской деятельности делает лиц, находящихся в

что чувствуют себя объектом необоснованного наблюдения со стороны полиции и испытывают негативные взаимодействия с полицией, которые, по их мнению, соответствуют существующей практике. расового профилирования»: доклад независимого эксперта по вопросам меньшинств: Addendum: Mission to Canada (8 March 2010), A/HRC/13/23/Add.2, at para 53 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/118/60/PDF/G1011860.pdf?OpenElement>.

[1186] See discussion in Section 5.4.2. («Algorithmic Bias and «Feedback Loops of Injustice").

[1187] See e.g., United Nations, Committee on the Elimination of Racial Discrimination, «Consideration of reports submitted by States parties under article 9 of the Convention" CERD/C/CAN/21-23 (8 June 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/114/64/PDF/ G1611464.pdf?OpenElement>.

[1188] See Section 2.1 («Criminal Justice and Systemic Discrimination in Canada").

[1189] See Section 2.2 («Bias and Inaccuracies in Police Data").

[1190] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 15.

[1191] This term is taken from Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: St. Martin's Press, 2018) at 7.

неблагоприятном социально-экономическом положении, особенно уязвимыми для ошибочного и непропорционального захвата системой уголовного правосудия. Такой захват возникает из-за «гипервидимости» данных, которая сама по себе является результатом более частого взаимодействия с государственными системами; эта гипервидимость также является следствием криминализации бедности и бездомности. В разделе 5.4.4 обсуждается, как технологии алгоритмического контроля могут включать в себя «неравенство по замыслу», одновременно скрывая системную несправедливость под видом научной и математической легитимности. Раздел 5.4.5 завершается кратким обсуждением и рекомендациями, извлечёнными из результатов и анализа разделов с 5.4.1 по 5.4.4.

5.4.1. Межсекторальный подход к равенству и свободе от дискриминации

Право на равенство и свободу от дискриминации - краеугольный камень международного права прав человека. МПГПП предусматривает, что «все люди равны перед законом и имеют право без какой-либо дискриминации на равную защиту закона».[1192] Государства также должны уважать и обеспечивать, чтобы права, закреплённые в Конвенции, были гарантированы всем лицам «без какого-либо различия, такого как раса, цвет кожи, пол, язык, религия, политические или иные взгляды, национальное или социальное происхождение, собственность, рождение. или другой статус».[1193]Государства также должны уважать и обеспечивать, чтобы права, закрепленные в Конвенции, были гарантированы всем лицам «без какого-либо различия, такого как раса, цвет кожи, пол, язык, религия, политические или иные взгляды, национальное или социальное происхождение, собственность, рождение или другой статус[1194] Право на равенство и право на свободу от дискриминации также гарантируется Хартией и квазиконституционными федеральными и провинциальными

[1192] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/ pages/ccpr.aspx>, art 26.

[1193] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/ pages/ccpr.aspx>, art 2.1.

[1194] See the International Covenant on Economic, Social and Cultural Rights (ICESCR), 19 December 1966, ratified by Canada 1976, 993 UNTS 3, Can TS 1976 No 46, 6 ILM 360, entered into force 3 January 1976, ratified by Canada 1976, <https://www.ohchr.org/en/professionalinterest/ pages/cescr.aspx>; International Convention on the Elimination of All Forms of Racial Discrimination, December 21, 1965, 660 UNTS 195 ratified by Canada in 1970, <https://www.ohchr.org/en/professionalinterest/pages/cerd.asx>; Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), adopted December 18, 1979, GA res 34/180, 34 UN GAOR Supp (No 46) at 193, UN Doc A/34/46, entered into force September 3, 1981, ratified by Canada 1981, <https://www.ohchr.org/en/professionalinterest/pages/cedaw.aspx>; Convention on the Rights of Persons with Disabilities (CRPD), adopted December 13, 2006, GA Res 61/106, Annex I, UN GAOR, 61st Sess, Supp (No 49) at 65, UN Doc A/61/49 (2006), entered into force May 3, 2008, <https://www.ohchr.org/en/hrbodies/crpd/pages/crpdindex.aspx>; Convention relating to the Status of Refugees, 189 UNTS 150, entered into force April 22, 1954, ratified by Canada on 4 June 1969.

кодексами прав человека, а также провинциальной Charte des droits et libertes de la personne (Хартии прав и свобод человека) в Квебеке.[1195]В разделе 15 Хартии говорится: «Все люди равны перед законом и имеют право на равную защиту и равные преимущества со стороны закона без дискриминации и, в частности, без дискриминации по признаку расы, национального или этнического происхождения, цвета кожи, религия, пол, возраст, умственные или физические недостатки».[1196]Защищает людей на основе характеристик, изложенных в положении выше, известных как по перечисленным основаниям, так и по аналогичным основаниям.[1197]

Верховный суд Канады признал следующие характеристики в качестве аналогичных оснований для конституционной защиты в соответствии с разделом 15: статус гражданства, семейное положение, сексуальная ориентация и аборигенность – место жительства.[1198] Этот список не обязательно является исчерпывающим, и в будущих случаях могут быть добавлены новые аналогичные основания. Действия правительства нарушают раздел 15 Хартии, если они имеют целью или следствием создание различия, основанного на перечисленных или аналогичных признаках, и это различие увековечивает невыгодное положение.[1199]Доказательство намерения провести дискриминацию не требуется; Защита по разделу 15 применяется до тех пор, пока закон или правительственная деятельность имеют дискриминационные последствия, независимо от намерений.[1200] Незаконная дискриминация может происходить косвенно через процесс, известный как «дискриминация неблагоприятных последствий» или «дискриминация неблагоприятных воздействий». Дискриминация в результате неблагоприятных воздействий определяется как «нейтральные правила с неблагоприятными последствиями для определенных групп».[1201] Теоретически такие правила нейтральны, но не с точки зрения их

[1195] See e.g., Canadian Human Rights Act, RSC 1985, c H-6; Human Rights Code, RSBC 1996, c 210; Human Rights Code, RSO 1990, c H.19; Alberta Human Rights Act, RSA 2000, c A-25.5; Charte des droits et libertes de la personne, RLRQ c C-12.

[1196] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, s 15(1).

[1197] Аналогичными основаниями являются те, которые прямо не перечислены в Уставе, но которые также "служат основой для стереотипных решений, принимаемых не на основе достоинств, а на основе личностной характеристики, которая является неизменной или изменчивой только при неприемлемых издержках для личной идентичности": Корбьер против Канады (министр по делам Индии и Севера), [1999 год] 2 SCR 203 по пункту 13.

[1198] Government of Canada, Department of Justice, «Section 15 - Equality Rights" <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/ check/art15.html>.

[1199] Kahkewistahaw First Nation v Taypotat, 2015 SCC 30 at para 16; R v Kapp, [2008] 2 SCR 483; Andrews v Law Society of British Columbia, [1989] 1 SCR 143; Law v Canada (Minister of Employment and Immigration), [1999] 1 SCR 497.

[1200] R v Kapp, [2008] 2 SCR 483; Andrews v Law Society of British Columbia, [1989] 1 SCR 143; Law v Canada (Minister of Employment and Immigration), [1999] 1 SCR 497.

[1201] Stewart v Elk Valley Coal Corp, 2017 SCC 30, at paras 80-81. Например, закон, который (гипотетически) санкционировал подчинение распознаванию лиц для доступа к государственным услугам - "нейтрально", потому что он применяется ко всем лицам - в действительности увековечил бы вредный недостаток для расированных людей с более темной кожей, чьи лица, как показали исследования, могут быть обнаружены не

применения или результатов. Основной вдохновляющий принцип раздела 15 – равенство, по существу. Фактическое равенство признаёт, что «любое различие в обращении между людьми в соответствии с законом не обязательно приведёт к неравенству, а также, что идентичное обращение может часто приводить к серьёзному неравенству».[1202]Соображения существенного равенства особенно уместны, когда речь идет о вводящем в заблуждение представлении о том, что алгоритмы «нейтральны», хотя на самом деле алгоритмы представляют собой яркие примеры дискриминации в связи с неблагоприятными последствиями.[1203] Жесткое формальное равенство математических формул вряд ли будет работать в контексте существенного неравенства, например, в системе уголовного правосудия, которая уже страдает от исторической и системной дискриминации.

Таким образом, при оценке алгоритмических инструментов полицейской деятельности, «чтобы приблизиться к идеалу полного равенства перед законом и под ним главным соображением должно быть воздействие закона на отдельного человека или группу». [1204]

Оценка этого воздействия в контексте технологии алгоритмического контроля требует межсекторального подхода.[1205]Такой подход признает, что «категории дискриминации могут пересекаться, [и] отдельные лица могут подвергаться исторической изоляции [на основании и] противостояния многочисленных причин неблагоприятного положения». Пересечение признаков дискриминации может привести к «особо сложным» жизненным ситуациям.[1206] «Отнесение такой дискриминации к [например] в первую очередь, расовой или в первую очередь, гендерной, неправильно понимает

точно или вообще в зависимости от того, как была разработана технология распознавания лиц: Joy Buolamwini, «When the Robot Doesn't See Dark Skin", New York Times (21 June 2018) <https:// www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html>. For examples of adverse discrimination cases, see e.g., Symes v Canada, [1993] 4 SCR 695 (child care expenses); Bliss v Attorney General of Canada, [1979] 1 SCR 183 (pregnancy); Brooks v Canada Safeway Ltd, [1989] 1 SCR 1219 (pregnancy); Kahkewistahaw First Nation v Taypotat, 2015 SCC 30 (education level); and Eldridge v British Columbia (Attorney General), [1997] 3 SCR 624 (hearing disability).

[1202] Andrews v Law Society of British Columbia, [1989] 1 SCR 143 at 164; Law v Canada (Minister of Employment and Immigration), [1999] 1 SCR 497; Kahkewistahaw First Nation v Taypotat, 2015 SCC 30, at para 17.

[1203] See e.g., Jeffrey Dastin, «Amazon scraps secret AI recruiting tool that showed bias against women", Reuters (9 October 2018) <https:// www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>; Adi Robertson, «Facebook's ad delivery could be inherently discriminatory, researchers say", Verge (4 April 2019), <https:// www.theverge.com/2019/4/4/18295190/facebook-ad-delivery-housing-job-race-gender-bias-study-northeastern-upturn> («A new study says that Facebook's ad delivery algorithm discriminates based on race and gender, even when advertisers are trying to reach a broad audience. The research backs up a similar claim that the US Department of Housing and Urban Development made last week when it sued Facebook for breaking housing discrimination laws."); and Claire Cain Miller, «When Algorithms Discriminate", New York Times (9 July 2015) <https://www. nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html>.

[1204] Andrews v Law Society of British Columbia, [1989] 1 SCR 143 at 165; R v Kapp, [2008] 2 SCR 483 at para 15.

[1205] The Supreme Court of Canada has recognized that some grounds of discrimination are embedded in, or intersect with others: Law v Canada, [1999] 1 SCR 497 at para 94.

[1206] Canada (Attorney General) v Mossop, [1993] 1 SCR 554 at 645-646 (L'Heureux-Dube J, in dissent).

реальность дискриминации, которую испытывают отдельные люди».[1207] Межсекторный анализ «делает акцент на реакции общества на человека в результате стечения обстоятельств, и он не требует деления человека по жестким критериям или категориям».[1208] Устранение нарушений прав на равенство с помощью технологий и обеспечение свободы от дискриминации с учётом всех нюансов взаимосвязанных аспектов необходимы для принятия эффективных ответных мер - правовых, нормативных или иных - которые учитывают коренные причины дискриминации и системного угнетения в системе уголовного правосудия Канады. Такая перспектива включает признание того, что «дискриминация эволюционировала и, как правило, больше не является явной, а становится более тонкой, многоуровневой, системной, экологической и институциональной».[1209] Таким образом, интерсекциональность особенно необходима при анализе индивидуальных и системных воздействий институционального внедрения технологии алгоритмической полицейской деятельности.

Раздел 15 Хартии применяется к алгоритмической полицейской деятельности, поскольку полиция является государственным субъектом, а деятельность полиции, поведение сотрудников и политика правоохранительных органов подпадают под «применение или действие закона», который запрещает дискриминацию в Хартии.[1210] Лица и сообщества, которые уже наиболее сильно пострадали от системы уголовного правосудия и которые предположительно по-прежнему больше всего страдают, в том числе от алгоритмического контроля, группы из защищенных согласно разделу 15 групп, которые исторически чрезмерно контролировались и несоразмерно криминализовались, которых заставляли молчать, наблюдало и контролировало государство. Эти сообщества определяются защищаемыми характеристиками, основанными на перечисленных или аналогичных признаках, такими как раса, сексуальная ориентация, коренная принадлежность или психическая инвалидность. Законодательство о правах человека также охватывает правоохранительную

[1207] Justice L 'Heureux-Dube пишет для меньшинства в Канаде (AG) против Моссопа, [1993] 1 SCR 554 at 645-646 (Mossop), цитируется в Комиссии по правам человека Онтарио: "Межсекторальный подход к дискриминации: рассмотрение множественных оснований в исках о правах человека" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move-towards- intersectional-approach>.

[1208] Ontario Human Rights Commission, «An intersectional approach to discrimination: Addressing multiple grounds in human rights claims" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move- towards-intersectional-approach>.

[1209] Ontario Human Rights Commission, «An intersectional approach to discrimination: Addressing multiple grounds in human rights claims" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move- towards-intersectional-approach>.

[1210] См., например, Elmardy v Toronto Police Services Board, 2017 ONSC 2074 (обнаружение нарушения раздела 15 на основе действий отдельной полиции, включая расовое профилирование и физическое нападение на истца); и Доу против столичного Торонто (муниципалитет) комиссаров полиции, 39 ОШ (3d) 487, 160 DLR (4) 697, 126 CCC (3d) 12 (вывод о нарушении раздела 15 на основании решения полицейской службы не предупреждать женщин, которым угрожает нападение со стороны серийного насильника, из-за веры в мифы об изнасиловании и сексистские стереотипы о женщинах).

деятельность [1211] и защищает маргинализованные группы от дискриминации, таким образом, будет также применяться там, где алгоритмическая полицейская деятельность влияет на право на равенство или свободу от дискриминации.[1212] Например, раздел 15 и законодательство о правах человека, вероятно, будут применяться в тех случаях, когда политика охраны правопорядка основана на предвзятом алгоритме или когда алгоритмическое «прогнозирование» способствует дискриминации со стороны офицера в отношении члена маргинализованного сообщества. В конечном счёте, технология алгоритмической полицейской деятельности может привести к нарушениям раздела 15 по крайней мере тремя всеобъемлющими способами: во-первых, путем увековечения дискриминационных циклов обратной связи и предвзятости подтверждения, что приводит к дальнейшей непропорциональной проверке со стороны полиции на сообществах, защищённых разделом 15; во-вторых, сделав группы, защищённые согласно разделу 15, особенно уязвимыми для правоохранительных действий в силу «гипервидимости данных»; и, в-третьих, через институционализацию и сокрытие основных причин системной дискриминации в уголовном правосудии, ограничивая при этом способность непосредственно бороться с ними. В следующих разделах отчета (с 5.4.2 по 5.4.4) каждый из этих вопросов рассматривается по очереди с заключительными комментариями в разделе 5.4.5.

5.4.2. Алгоритмический уклон и «петли обратной связи несправедливости»

Использование правоохранительными органами алгоритмической полицейской технологии потенциально нарушает раздел 15, где использование технологии приводит к тому, что защищенные группы подвергаются неравной защите со стороны закона или теряют равные преимущества закона. Как и в случае с традиционными методами полицейской деятельности, в случае алгоритмической полицейской деятельности «применение или действие закона» происходит через действия, политику и поведение полиции. Алгоритмическая предвзятость в технологиях охраны правопорядка может привести к неравенству и увековечить невыгодное положение групп, защищенных согласно разделу 15. Такое увековечение является результатом

[1211] «Консенсус в отношении нескольких случаев, охватывающих более трех десятилетий антидискриминационного законодательства, заключается в том, что правоохранительной деятельностью муниципальных и региональных полицейских сил являются" государственные службы "или" учреждения "[, как они определены в законодательстве о правах человека]". Justice Walter Surma Tarnopolsky, Discrimination and the Law, 1st ed (Toronto: Carswell, 2004) (loose-leaf updated 2020) at ch 11 at 11.6(c) («Municipal Police").

[1212] В отношении примеров действий полиции, признанных дискриминационными в соответствии с законодательством о правах человека, see e.g., Hum v Royal Canadian Mounted Police, 8 CHRR D/3748; Johnson v Halifax Regional Police Service, [2003] NSHRBIDNo 2, 48 CHRR D/307; and Dawson v Vancouver Police Board, 2015 BCHRT 54.

увеличения предвзятости подтверждения и дискриминационных петель обратной связи, которые возникают, когда проблемные данные полиции используются для обучения алгоритмов полицейской деятельности.[1213] Эта форма алгоритмической предвзятости может несправедливо усилить и без того повышенное внимание, подозрительность со стороны полиции и агрессию по отношению к членам маргинализованных сообществ, усугубляя ранее существовавшую дискриминацию.

В результате группы, защищенные статьей 15, теряют «равную выгоду» и «равную защиту» закона, включая другие права Хартии, такие как презумпция невиновности,[1214] право на свободу от необоснованного обыска и изъятия[1215] и право не подвергаться произвольному задержанию.[1216]

При отсутствии контроля такое положение дел нанёсет ущерб автономии и достоинству этих сообществ и отдельных лиц в них. В оставшейся части этого подраздела мы подробно рассмотрим каждый из вышеперечисленных пунктов по очереди. Алгоритмическая предвзятость и дискриминационные петли обратной связи возникают, когда дискриминационные шаблоны в полицейских данных встроены в полицейские алгоритмы, которые были обучены на таких данных, и закреплены ими.[1217]Исторический недостаток и адресность защищенных групп раздела 15 встроены в данные и, следовательно, встроены в сами алгоритмы. Как пишут Особа и Велсер, «применение процедурно правильных алгоритмов к смещённым данным - хороший способ научить искусственных агентов имитировать любые смещения, содержащиеся в данных».[1218]Алгоритмы, которые обучаются на полицейских данных, часто состоящих из грязных данных,[1219] таким образом, вероятно, будут выявлять, включать и воспроизводить исторические модели дискриминации в результате нарушения прав защищённых групп, закреплённых в разделе 15, путем предоставления им меньшей правовой защиты от поведения государства.

Например, в исследовании 2019 года Рашида Ричардсон, Джейсон Шульц и Кейт Кроуфорд продемонстрировали, что по крайней мере девять юрисдикций в Соединенных Штатах, вероятно, обучили модели прогнозной полицейской деятельности с использованием полицейских данных, полученных

[1213] See the discussion in Section 2.2 («Bias and Inaccuracies in Police Data").
[1214] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, section 11(d).
[1215] See Section 5.2 («Right to Privacy").
[1216] See Section 5.5 («Right to Liberty and to Be Free from Arbitrary Detention").
[1217] See the discussion in Section 2.2 («Bias and Inaccuracies in Police Data").
[1218] Osonde Osoba & William Welser IV, «An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence", RAND Corporation (2017) at 17 <https://pdfs.semanticscholar.org/b7be/0be36706c30a76312b34d60ff02d97698191.pdf>.
[1219] См. раздел 3.1 ("Технический букварь"): "В тех случаях, когда алгоритм работы полиции был загрязнен поврежденными, искаженными, неполными или предвзятыми данными (непреднамеренно или намеренно), он был обучен работе с грязными данными".

в периоды, когда проводились «правительственные расследования, постановления о согласии или другие документы о коррумпированных, расовых или иных незаконных действиях полиции».[1220] Ричардсон и др. обнаружили «веские доказательства» и «чрезвычайно высокую вероятность» того, что системы прогнозирования полиции Чикаго и Нового Орлеана, соответственно, были построены на этих «грязных данных».[1221] Авторы исследования заявили, что, в дополнение к другим «исследованиям, которые эмпирически демонстрируют, что математические модели систем прогнозирования полицейской деятельности подвержены неконтролируемым циклам обратной связи»,[1222]их собственные результаты показали, что «петли обратной связи также являются побочным продуктом предвзятых данных полиции».[1223]Обе исследовательские группы обнаружили, что петли обратной связи означают, что полицию «неоднократно отправляли обратно в одни и те же районы независимо от фактического уровня преступности».[1224]

В отдельном исследовании оценка алгоритма PredPol Лумом и Исааком применительно к преступлениям, связанным с наркотиками в Окленде, штат Калифорния, показала, что « нехватка чернокожих людей станет мишенью для прогнозирующей полиции примерно в два раза чаще, чем белых», несмотря на то, что «примерно эквивалентное» употреблению наркотиков.[1225] Алгоритм также был нацелен на домохозяйства с низкими доходами по «непропорционально высоким показателям».[1226]

Грязные данные могут также появиться в контексте канадской полиции. Такие данные могут быть получены в результате институциональной или бессознательной предвзятости, прямо или косвенно дискриминационной политики и практики или неправомерных действий полиции. Многочисленные исследования, запросы, судебные решения и расследования показали, что, например, чернокожие и коренные народы чрезмерно представлены в данных о кардинге, уличных проверках, арестах, предварительном заключении,

---

[1220] Rashida Richardson, Jason M Schultz & Kate Crawford, «Dirty Data, Bad Predictions: How civil rights violations impact police data, predictive policing systems, and justice" (May 2019) 94:192 New York University Law Review 192 at 197 <https://www.nyulawreview.org/wp- content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>.

[1221] Эти доказательства появились, в частности, в результате "обширной грязной полицейской практики и повторного судебного разбирательства". В случае графства Марикопа были затронуты также соседние юрисдикции, поскольку в них использовались те же полицейские данные и инструменты, которые включали или основывались грязных данных. Ibid at 204.

[1222] Ibid at 218. Richardson, Schultz, and Crawford cite Danielle Ensign et al, «Runaway Feedback Loops in Predictive Policing" (2018) 81:1 Proceedings of Machine Learning Research <https://arxiv.org/pdf/1706.09847.pdf>; see also Kristian Lum & William Isaac, «To predict and serve?" (2016) 13:5 Significance 14.

[1223] Ibid.

[1224] Ibid.

[1225] Kristian Lum & William Isaac, «To predict and serve?" (2016) 13:5 Significance 14 at 18; for critiques and defence of this study, see William Isaac & Kristian Lum, «Setting the Record Straight on Predictive Policing and Race", The Medium (3 January 2018) <https://medium.com/in- justice-today/setting-the-record-straight-on-predictive-policing-and-race-fe588b457ca2>.

[1226] Ibid.

приговорах и заключении под стражу, и что такое чрезмерное представительство является результатом предвзятости практики уголовного правосудия или системной дискриминации.[1227]Кроме того, существуют предвзятые данные о других маргинализированных группах, таких как ЛГБТК, и они влияют на них,[1228] людей с психическими заболеваниями,[1229]и на сообщества с низкими доходами.[1230]

Данные полиции также могут отражать, что системная дискриминация приводит к недостаточному контролю над полицейскими,[1231] включая отсутствие полиции там, где это необходимо (и отмечая, что усиление присутствия полиции отличается от увеличения количества полицейских остановок в сообществе) исторически маргинализированных сообществ, где они становятся жертвами преступлений. Например, Джонатан Рудин написал в отчёте, подготовленном для расследования Иппервоша, «аборигены чрезмерно представлены в системе уголовного правосудия не только как обвиняемые, но и как жертвы. [Они] часто рассматриваются полицией как менее достойные

[1227] См., например, раздел 2.1 ("Уголовное правосудие и системная дискриминация в Канаде"). См. также: "В период с 2008 по 2013 год вероятность появления [чернокожих] в наборе данных контактных карточек в три раза выше, чем их представительство в населении": Комиссия по правам человека Онтарио, под подозрением: Доклад об исследованиях и консультациях по расовому профилированию в Онтарио (апрель 2017 года) по адресу: at 37 <http://www.ohrc.on.ca/en/under-suspicion- research-and-consultation-report-racial-profiling-ontario>.

[1228]Например, Джон Фишер подробно рассказывает о том, как некоторые положения Уголовного кодекса, такие, как правонарушения, связанные с непристойностью или непристойностью, часто применялись таким образом, что это приводило к дискриминации ЛГБТК и их общин, практики и учреждений. John Fisher, «Outlaws or In-laws?: Successes and Challenges in the Struggle for LGBT Equality", (2004) 49 McGill Law Journal 1183 at 1201¬1202 (footnotes omitted) <https://lawjournal.mcgill.ca/wp-content/uploads/pdf/449577-4fishe.pdf> («Как и положения о "непристойности" в таможенном режиме, критерий "непристойности" в "бардачке" является нейтральным на лице, субъективным в его применении, зависит от "общинных стандартов терпимости" и используется для воздействия на учреждения и практику ЛГБТ. [...] Нет никаких сомнений в том, что полицейские облавы на "причуды", такие как гей-баня, представляют собой фундаментальное посягательство на нашу идентичность и консенсусное выражение нашей сексуальности ". Police institutions have also historically played a significant role in the persecution of LGBTQ communities in Canada, such as in the 1981 Toronto bathhouse raids. See e.g., Jamie Bradburn, «Historicist: Raiding the Bathhouses", Torontoist (23 May 2015) <https://torontoist.com/2015/05/historicist-raiding-the- bathhouses>; and Michael Gold and Derek M Norman, «Stonewall Riot Apology: Police Actions Were 'Wrong,' Commissioner Admits", New York Times (6 June 2019) <https://www.nytimes.com/2019/06/06/nyregion/stonewall-riots-nypd.html>.

[1229] See generally Glen Luther & Mansfield Mela, «Mental Illness and Sentencing: Blaming the Mentally Ill for their Lack of Cooperation with Inadequate Treatment in R v Maier», ABlawg (30 March 2015) <https://ablawg.ca/wp-content/uploads/2015/03/Blog_GL_MM_Maier_ March2015.3.pdf>; The Honourable Justice Richard D Schneider, «The Mentally Ill: How They Became Enmeshed in the Criminal Justice System and How We Might Get Them Out", Department of Justice: Research and Statistics Division (March 2015) <https://www.justice.gc.ca/eng/rp-pr/jr/mental/mental.pdf>; Roslyn Shields, «Mental Health and Criminal Justice Policy Framework", Centre for Addiction and Mental Health (October 2013) <https://www.camh.ca/-/media/files/pdfs---public-policy-submissions/mh_criminal_justice_policy_framework-pdf.pdf>; and Tanya Dupuis, Robin MacKay & Julia Nicol, «Current Issues in Mental Health in Canada: Mental Health and the Criminal Justice System", Library of Parliament Background Paper (16 December 2013) <https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/BackgroundPapers/PDF/2013- 88-e.pdf>.

[1230] See Section 5.4.3 («Socioeconomic Disadvantage and Hypervisibility to Algorithmic Policing").

[1231] «Недостаточная работа полиции, как правило, связана с неадекватными мерами правоохранительных органов по борьбе с виктимизацией или вероятной виктимизацией какого-либо лица или группы лиц. Например, уже давно существуют проблемы, связанные с недостаточной охраной правопорядка в связи с сексуальными нападениями на женщин и насилием в отношении ЛГБТК + общин. "Ontario Human Rights Commission, «Policy on eliminating racial profiling in law enforcement" (20 June 2019) , at 2.2 (footnotes omitted) <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

жертвы, и поэтому просьбы о помощи часто игнорируются или преуменьшаются. [...] Недостаточный контроль и чрезмерный контроль — это две стороны одной медали».[1232] Комиссия по правам человека Онтарио признает недополучение расовых лиц формой расовой дискриминации, которая имеет место как индивидуально среди конкретных сотрудников правоохранительных органов, так и институционально в рамках системного реагирования на преступления, затрагивающие, в частности, представителей чернокожих, коренных или расовых общин. [1233]Сообщество ЛГБТК также исторически получало неравную и меньшую «защиту закона», например, в 2018 году, когда полицейские службы, казалось, не спешили расследовать дело серийного убийцы, нацелившегося на гей-деревню Торонто.[1234]Алгоритмы, обученные на грязных данных, отражают динамику, лежащую в основе первоначального сбора данных, и, таким образом, создают неблагоприятные условия для затронутых лиц и групп с защищёнными характеристиками. Например, системная предвзятость из-за недостаточного контроля может привести к получению грязных данных, которые используются для обучения полицейских алгоритмов, что увековечивает предвзятость за счёт систематической и значительной недооценки степени, в которой члены маргинализированных сообществ становятся жертвами преступников. Алгоритмы применения политик, которые обучаются на грязных данных, также могут отражать недостаточное использование политик, [1235] где к

[1232] Jonathan Rudin, Aboriginal Peoples and the Criminal Justice System (Toronto: Ipperwash Inquiry, 2005) at 1-2, Ipperwash Inquiry <www. attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/research/pdf/Rudin.pdf>. Кроме того, Комиссия по правам человека Онтарио заявила: "В заключительном докладе Национального расследования по вопросу о пропавших без вести и убитых женщинах и девочках из числа коренных народов излагаются исторические, культурные и политические аспекты недостаточной полицейской деятельности. Расовая дегуманизация является повторяющейся темой, и во многих случаях термин "одноразовый" используется для обозначения того, как доминирующее общество часто относится к женщинам и девочкам из числа коренных народов." Ontario Human Rights Commission, «Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2.1 <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

[1233] Ontario Human Rights Commission, «Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2 <http://www.ohrc. on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

[1234] Смотрите, например, "Виджаянатхан, который является одним из самых откровенных критиков того, как Торонто подвел свое гей-сообщество, настаивает, что полиция серьезно отнеслась к расследованиям только тогда, когда Эндрю Кинсман, один из двух белых жертв, был объявлен пропавшим без вести. Но он также указывает на расизм в гей-сообществе - сравнивая массовые местные обыски, проведенные после исчезновения другой белой жертвы... с более медленной и менее последовательной реакцией на исчезновения коричневокожих жертв." David Graham, «How alleged Toronto serial killer Bruce McArthur went unnoticed", Guardian (23 June 2018) <https://www.theguardian.com/world/2018/jun/23/bruce-mcarthur-toronto-gay-serial-killer>. The article later quotes historian Tom Hooper: «For both gay men in the 1970s and queer people of colour today, the police have been enforcers but not protectors. Isolation, combined with a fear of police, has marginalized members of our community and made them more vulnerable to violence."

[1235]Помимо практики пренебрежения по отношению к жертвам преступлений из числа коренного населения и расовых преступлений, недостаточная охрана порядка может принимать совершенно иную форму - фаворитизм по отношению к классу-нарушителю. " Учитывая ограниченность ресурсов правоохранительных органов, расовое профилирование как проявление чрезмерной полицейской деятельности, направленной против коренного населения и расово настроенного населения, может повлечь за собой недостаточную полицейскую деятельность в отношении белых людей, которые занимаются преступной деятельностью. УЛР описывает эти специфические для расы модели правоприменения как преференциальное недержание полиции. Это, пожалуй, чаще всего иллюстрируется в области обеспечения соблюдения законов о наркотиках. " Комиссия по правам человека Онтарио, "Политика ликвидации расового профилирования в правоохранительных органах" Ontario

правонарушителям из доминирующих социальных слоев относятся более снисходительно или благосклонно со стороны правоохранительных органов – как инструмент оценки рисков COMPAS, так и алгоритм PredPol в Lum и где правоохранительные органы обращаются с правонарушителями из доминирующих социальных классов более снисходительно или благоприятно – оба инструмента оценки риска COMPAS и алгоритм PredPol в исследовании Лам и Айзек привёл к непропорционально благоприятному обращению с белыми правонарушителями.

В конечном итоге полицейские данные, которые не отсеивают слои предвзятости по отношению ко всем затронутым группам, защищённым разделом 15, будут представлять собой грязные данные, и их не следует использовать для обучения алгоритмов с целью полицейской деятельности, обеспечения правопорядка, исправлений или других функций системы уголовного правосудия.

Использование распознавания лиц канадскими полицейскими службами вызывает особую озабоченность по поводу обратной связи. В Калгари и Торонто, например, полицейские системы распознавания лиц облегчают идентификацию неизвестных лиц путём поиска их изображений по базам данных полицейских фотографий. В результате людей, которым ранее были предъявлены обвинения, но которые являются юридически невиновными, или тех, кто был осуждён за уголовное преступление, может быть легче или ошибочно идентифицировать, учитывая высокий уровень ошибок технологии распознавания лиц,[1236] в будущем, чем те, кому ранее не было предъявлено обвинение или суд.[1237] Программы распознавания лиц могут подвергать охраняемые Хартией группы непропорционально высокому уровню подозрений и проверок со стороны полиции по сравнению с лицами, которые не были зафиксированы в базах данных о фотографиях, или которые принадлежат к группам, которые исторически не подвергались преследованиям

Human Rights Commission, «Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2 (footnotes omitted) <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

[1236] See Section 5.2.4 («Data Accuracy: Inaccurate Data and Inaccurate Algorithms").

[1237] «Как только подозреваемый находится в базе данных, он может неоднократно подвергаться слежке; правоохранительные органы могут проводить ретроактивный поиск данных ALPR и идентифицировать лиц, транспортные средства, время и места, а не начинать собирать информацию о них только после того, как они попадут под подозрение." Sarah Brayne, «Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Rev 977 at 1000. This is even before taking into account facial recognition systems such as Clearview AI, which scrapes photos from social media data across the entire web, and which has been tested by police services in Toronto, Peel, and Halton, Ontario. Kashmir Hill, «The Secretive Company That Might End Privacy as We Know It", New York Times (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; «Toronto police admit using secretive facial recognition technology Clearview AI", CBC News (13 February 2020) <https://www.cbc.ca/news/canada/toronto/toronto-police-clearview- ai-1.5462785>; and Wendy Gillis & Kate Allen, «Peel and Halton police reveal they too used controversial facial recognition tool", Toronto Star (14 February 2020) <https://www.thestar.com/news/gta/2020/02/14/peel-and-halton-police-reveal-they-too-used-controversial-facial-recognition- tool.html>.

и по-прежнему не являются объектами преследования.[1238] Такая непропорциональная и неоправданная проверка будет представлять собой увековечение неблагоприятного положения по перечисленным или аналогичным основаниям в нарушение права на равенство, закреплённого в Хартии. Некоторые сотрудники канадских правоохранительных органов признали потенциал прогнозирующей полицейской деятельности для закрепления дискриминационных петель обратной связи. Сотрудник правоохранительных органов в Калгари заявил: «Мы можем увидеть, ведём ли мы активную работу в определённых областях, которая исказит данные. Мы будем получать больше звонков туда, потому что мы отправили туда людей».[1239] Департамент полиции Ванкувера (VPD) попытался смягчить потенциальную предвзятость, исключив инциденты, о которых сообщают полицейские, из своих алгоритмических прогнозов преступности, и оно обучает алгоритмы GeoDASH исключительно на данных проверенных взломов и проникновений, о которых сообщают представители общественности. [1240]Однако некоторые формы предвзятости, в том числе тот факт, что некоторые общины с большей вероятностью будут сообщать о преступлениях в полицию, чем другие, или более вероятно, что полиция будет серьезно относиться к ним при сообщении о преступной деятельности, может остаться, несмотря на такие усилия.[1241]

Предупреждающий блок, отслеживающий, что их район был идентифицирован алгоритмом как потенциальное место преступной деятельности, также может вызвать эффект «неуместности», когда жители или правоохранительные органы дискриминируют людей, склонных к расе, в преимущественно белых или более богатых районах.[1242]

[1238] См. раздел "IN FOCUS # 5: Технология распознавания лиц и эрозия прав на конфиденциальность" в разделе 5.2.4 ("Точность данных: неточные данные и неточные алгоритмы").

[1239] Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

[1240] Я не хотел иметь никаких данных, которые могли бы быть восприняты как предвзятое отношение полиции с точки зрения генерации звонков. Всегда есть представления, что полиция может в основном разворачиваться в районах, где у них есть предвзятое представление о том, что существует более высокая степень преступности из-за этнического, социально-экономического статуса, или любого из тех основных вопросов, которые могут предрасполагать полицейских к поездке в определенные районы. И исходя из этого, это может быть самоисполняющееся пророчество. И затем они обнаруживают преступления, потому что, если вы сосредотачиваете все свои ресурсы, предварительно развертывая их на основе ваших собственных предубеждений, вы будете находить вещи, если вы их ищете. Я верю, что это правда или нет, что это происходит в полиции Ванкувера, я не хотел, чтобы призрак, который может даже войти в предвзятость данных. Исходя из этого, я принял решение, что мы будем использовать только публичные сообщения об имущественных преступлениях ". Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

[1241] See Section 2.2 («Bias and Inaccuracies in Police Data").

[1242] «Конкретные действия полиции, связанные с мониторингом дорожного движения, могут рассматриваться как формы системного расового профилирования. Одна из них заключается в том, чтобы остановить и допросить людей, которые считаются "неуместными", а не жителей района, в котором они находятся. Районы с более высоким уровнем дохода, как правило, заселяются белыми жителями. Это в сочетании со стереотипами, связывающими расово настроенных людей с преступностью, может привести к тому, что расово настроенные люди в этом районе с большей вероятностью будут остановлены, поскольку их считают подозрительными. ": Ontario Human Rights Commission, «OHRC Response to the Race Data and Traffic Stops in Ottawa Report" (28

Алгоритмическая ошибка может возникнуть, даже если явные маркеры защищённых характеристик, таких как раса, национальное происхождение или инвалидность, удалены из наборов данных. [1243]Такое смещение может возникать, потому что характеристики могут быть закодированы в прокси-данных, то есть данных, которые могут не относиться к типу, который может вызвать дискриминацию, но который коррелирует с информацией, которая действительно дает основания для защиты по разделу 15. Например, почтовые индексы в Соединенных Штатах часто связаны с расой.[1244] из-за расовой дискриминации исторической практики.[1245] Таким образом, использование почтовых индексов может служить прокси-сервером для гонки, что повышает защиту по разделу 15. Другие примеры прокси-данных включают использование поисковой активности человека в Интернете для определения расы, возраста и пола;[1246] использование «понравившихся» брендов или страниц на Facebook для определения расы;[1247] и используя историю покупок или публикаций в социальных сетях, чтобы сделать вывод о состоянии здоровья.[1248]

November 2016) <http://www.ontla.on.ca/library/repository/ mon/30012/337641.pdf>, at 3 (footnotes omitted); see also: «The Star analysis of the police stop data shows blacks are more likely than whites to be documented in areas where fewer black people live." Jim Rankin and Patty Winsa, «Known to police: Toronto police stop and document black and brown people far more than whites", Toronto Star (9 March 2012) <https://www.thestar.com/news/insight/2012/03/09/known_to_police_ toronto_police_stop_and_document_black_and_brown_people_far_more_than_whites.html>.

[1243] See e.g., Andrew D Selbst, «Disparate Impact in Big Data Policing", (2017) 52 Georgia Law Review 109 <https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2819182>; and Solon Barocas and Andrew D Selbst, «Big Data's Disparate Impact", (2016) 104 California Law Review 671, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899>.

[1244] В Канаде маркетинговые данные имеют схожую корреляцию, например, инструмент PRIZM5 Environics Analytics, который сортирует каждый канадский почтовый индекс в один из 68 "типов образа жизни" с профилями окрестностей, которые иногда указывают на расовый и социально-экономический статус. Эти профили районов включают такие названия, как "Искусство и достаток", "Азиатские изысканности", "Возрождение новичков", "Южноазиатское общество", "Нуво Рихес", "Семьи первых наций", "Анклавы многоэтнические", "Малоэтажные арендаторы" и "Южноазиатские достижения". Насколько могли бы убедиться авторы настоящего доклада, такого рода маркетинговые данные не используются для информирования алгоритмов полицейской работы в Канаде. «PRIZM5 Segment Snapshots 2015", <http://assets.cengage. com/training/AOD_PRIZM5_Snapshots.pdf>; see also «PRIZM5", Environics <downloads.esri.com/esri_content_doc/dbl/int/Environics-PRIZM5- Segment-Side.pdf>.

[1245] See e.g., Alexis Madrigal, «The Racist Housing Policy That Made Your Neighborhood", The Atlantic (22 May 2014) <https://www.theatlantic. com/business/archive/2014/05/the-racist-housing-policy-that-made-your-neighborhood/371439/>; Digital Chicago, «Racial Restriction and Housing Discrimination in the Chicagoland Area", <https://digitalchicagohistory.org/exhibits/show/restricted-chicago/other/redlining>; and Camila, Domonoske, «Interactive Redlining Map Zooms In On America's History Of Discrimination", NPR (19 October 2016) <https://www.npr.org/ sections/thetwo-way/2016/10/19/498536077/interactive-redlining-map-zooms-in-on-americas-history-of-discrimination>. Кроме того, некоторые явно воспользовались такими корреляциями, как, например, компания по подготовке тестов SAT The Princeton Review, которая процитировала более высокую цену за свою услугу "24-часового онлайн-репетиторства" для американских почтовых индексов с непропорционально более высоким населением Азии по сравнению с другими почтовыми кодами, которые были процитированы ниже цен на ту же услугу: Jeff Larson, Surya Mattu & Julia Angwin, «Unintended Consequences of Geographic Targeting", (September 2015) Technology Science <https://techscience.org/a/2015090103/>.

[1246] Sara Wachter-Boettcher, «Google Thought I Was a Man", Nautilus (28 September 2017) <nautil.us/issue/52/the-hive/google-thought-i-was- a-man>.

[1247] Julia Angwin & Terry Parris Jr, «Facebook Lets Advertisers Exclude Users by Race", Pro Publica (28 October 2016) <https://www.propublica. org/article/facebook-lets-advertisers-exclude-users-by-race>.

[1248] «Когда компьютеры поляка пролезли по данным, он смог идентифицировать около 25 продуктов, которые

В контексте полицейской деятельности Канады данные, которые, возможно, не казались проблематичными, когда они были собраны, используются для того, чтобы сделать выводы, которые могут привести полицейские органы к неверным выводам и могут быть приняты во вред пострадавшим лицам. Одним из примеров этого является определение того, является ли ученик членом банды, на основе его друзей в школе.[1249]Алгоритмическая предвзятость и дискриминирующие петли обратной связи, которые могут возникнуть из-за технологии алгоритмического контроля, могут привести к двум дополнительным последствиям, которые ещё больше усугубят невыгодное положение маргинализованных групп, защищённых в соответствии с разделом 15 Закона о защите прав. Во-первых, характеристика районов как «высокий уровень преступности» или отдельных лиц как «высокий риск» вызывает опасения, что алгоритмическое полицейское управление может вызвать излишнюю подозрительность и более агрессивное полицейское наблюдение в отношении идентифицированных лиц или лиц в определённых районах. Офицеры, которые патрулируют алгоритмически выделенные области или получают предупреждение о конкретных людях с помощью алгоритма, могут с большей вероятностью выполнить остановку или применить силу или чрезмерную силу по сравнению с теми же обстоятельствами без алгоритмической «подсказки».[1250] Неконституционные задержания уже происходят в Канаде без алгоритмического стимулирования подозрений, страха или агрессии среди полицейских. [1251]

Серьёзные последствия могут иметь место в случае, если районы или отдельные лица будут заранее помечены алгоритмическими «красными флажками», особенно там, где уже существует напряженность между правоохранительными органами и отмеченными сторонами. Чрезмерное применение силы правоохранительными органами уже несоразмерно наносит вред группам, защищаемым согласно разделу 15, в частности, общинам чернокожих и коренных жителей [1252] и лицам, имеющим психические

при совместном анализе позволили ему назначить каждому покупателю оценку" прогноз беременности ". Что более важно, он также мог оценить ее срок в течение небольшого окна, так что Target могла отправлять купоны, приуроченные к очень конкретным стадиям ее беременности ". Charles Duhigg, «How Companies Learn Your Secrets", New York Times Magazine (16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>; and Olga Khazan, «What Your Facebook Posts Say About Your Mental Health", Atlantic (6 November 2019) <https://www.theatlantic.com/health/archive/2019/11/what-your-tweets-say- about-your-mood/601510/>.

[1249] See discussion regarding gang databases, under Section 2.2 («Bias and Inaccuracies in Police Data").

[1250] Andrew Guthrie Ferguson, «Predictive Policing and Reasonable Suspicion" (January 2013) 62:2 Emory Law Journal 259 at 305-308.

[1251] See e.g., Elmardy v Toronto Police Services Board, 2015 ONSC 2952; R v Ohenhen, 2016 ONSC 5782; R v Schuhknecht, 2005 BCPC 161; and R v K(A), 2014 ONCJ 374.

[1252] See e.g., Scot Worley, «Police Use of Force in Ontario: An Examination of Data from the Special Investigations Unit: Final Report" (Research Project Conducted on behalf of the African Canadian Legal Clinic for Submission to the Ipperwash Inquiry) <https://www.attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/projects/pdf/AfricanCanadianClinicIpperwashProject_SIUStudybyScotWortley.pdf>; Ontario Human Rights Commission, A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service (November 2018)

расстройства.[1253] Исследования показали, что даже если алгоритмическая пометка не увеличивает вероятность физического насилия, «усиление контроля и наблюдения в результате непропорционального патрулирования сообществ, которые исторически чрезмерно охранялись, были связаны с ухудшением психического и физического здоровья».[1254] Алгоритмические технологии, которые могут продолжить или усилить исторические модели насилия в отношении членов маргинализованных сообществ, скорее всего, будут иметь дискриминационный характер, нарушая права равенства в разделе 15. Во-вторых, прогнозирующая полицейская работа и алгоритмическое наблюдение, которые имеют предполагаемый или фактический эффект необоснованного или непропорционального нападения на исторически маргинализированные сообщества, могут ухудшить автономию, достоинство, благополучие и отношения сообщества с полицейскими службами. Такая деградация,

---

<ohrc.on.ca/sites/default/files/TPS%20Inquiry_Interim%20Report%20EN%20FINAL%20DESIGNED%20for%20remed_3_0.pdf#overlay-context=en/news_centre/ohrc-interim-report-toronto-police-service-inquiry-shows-disturbing-results> at 30¬32; Farida Deif, «Submission to the Government of Canada on Police Abuse of Indigenous Women in Saskatchewan and Failures to Protect Indigenous Women from Violence" (June 2017) Human Rights Watch <https://www.hrw.org/sites/default/files/supporting_resources/canada_ saskatchewan_submission_june_2017.pdf>; The Honourable Michael H. Tulloch, Report of the Independent Police Oversight Review (2017) at 26¬27 and 223-25 <http://www.policeoversightreview.ca/ReportoftheIndependentPoliceOversightReview.pdf>; Ontario Human Rights Commission, Under Suspicion: Research and consultation report on racial profiling in Ontario (April 2017), at 42-43, 65, 104 <http://www.ohrc.on.ca/en/ under-suspicion-research-and-consultation-report-racial-profiling-ontario>; Anastassia Bystrova, «Does Suspect Race Influence Use of Force by Police?" (2016) 5:1 Sociological Imagination: Western's Undergraduate Sociology Student Journal 1 <https://ojs.lib.uwo.ca/index.php/si/article/ view/5310/4455>; and Andrew Russell, «Sask., Quebec arrest videos show 'startling' examples of excessive police force: experts", Global News (4 July 2019) <https://globalnews.ca/news/5456773/sask-quebec-arrest-videos-excessive-police-force-experts/>.

[1253] «Существует также социально значимая взаимосвязь между расовой принадлежностью и психическим здоровьем, которая может повлиять на решения офицеров о применении силы. Существуют стереотипы о чернокожих в отношении насилия и преступности, а также опасения, что полиция с большей вероятностью применит силу в своих контактах с чернокожими. Кроме того, лица, страдающие психическими расстройствами, могут с большей вероятностью подвергаться применению силы со стороны сотрудников из-за реагирования на инструкции или действия полиции, которые могут показаться необычными, непредсказуемыми или неуместными, или из-за того, что полиция полагается на стереотипные предположения об опасности или насилии. [...] " Ontario Human Rights Commission, A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service (November 2018) <ohrc.on.ca/sites/default/files/TPS%20Inquiry_Interim%20Report%20EN%20FINAL%20DESIGNED%20for%20remed_3_0.pdf#overlay-context=en/news_centre/ohrc-interim- report-toronto-police-service-inquiry-shows-disturbing-results> at 8 (footnote omitted). Читайте также "Дальнейший анализ показывает, что чернокожие гражданские лица чрезмерно представлены в случаях применения силы, в которых не было отмечено никакого кризиса психического здоровья.... Чернокожие гражданские лица также чрезмерно представлены в случаях применения силы СИУ, когда были выявлены проблемы с психическим здоровьем.... Белые гражданские лица, напротив, чрезмерно представлены в случаях применения силы, когда речь идет о гражданских лицах, которые были идентифицированы как находящиеся в кризисе психического здоровья, и недостаточно представлены в случаях, когда не было отмечено никаких проблем с психическим здоровьем. " Ibid at 94-95. See also R vForcillo, 2018 ONCA 402; and Katherine Wilton, «Video captures Montreal police fatally shooting mentally ill man", Montreal Gazette (1 March 2019) <https://montrealgazette.com/news/local-news/video-captures-montreal-police-fatally-shooting-mentally-ill-man>.

[1254] Hannah Couchman, «Policing by Machine: Predictive policing and the threat to our rights," Liberty (January 2019), at 17 (footnotes omitted). Далее в докладе говорится: "Это подтверждается другими исследованиями, которые показывают, что проживание в районах, где пешеходные остановки чаще становятся инвазивными, связано с ухудшением здоровья, и что количество сообщений о травмах и тревогах молодых людей в Нью-Йорке возросло по мере увеличения числа случаев контактов с полицией, особенно среди тех, кто сообщает о случаях вмешательства и/или несправедливых остановках полиции. Расширение контактов с полицией также создало дополнительные возможности для насилия со стороны полиции в перегруженных полицией районах. "

независимо от того, используются ли алгоритмические полицейские технологии, подрывает автономию и благополучие сообщества, обостряет ранее существовавшую напряжённость между полицией и сообществами, несоразмерно криминализированными, и подрывает репутацию отправления правосудия.

Развёртывание технологии алгоритмической полицейской деятельности для сосредоточения патрульных сил в районах, которые преимущественно населены группами, защищёнными разделом 15; отмечать маргинализированных лиц для более тщательного изучения до того, как будет совершено какое-либо нарушение; или для мониторинга их онлайн-разговоров и социальных сетей (особенно с учётом прав Хартии на свободу выражения мнений и собраний[1255]) воспроизведут общие и давние образцы системной дискриминации. Джонатан Рудин, юрист и программный директор Aboriginal Legal Services, высказал следующие личные взгляды, говоря только от своего имени, относительно алгоритмической работы полиции и её потенциального воздействия на маргинализированные сообщества: Если что-то должно быть сделано, должен быть уровень прозрачности, обмена информацией и обсуждения того, почему что-то делается. Вы не можете начать с того, что скажете: «Забудьте всё прошлое и давайте двигаться вперед». Если это основа для развертывания, они потерпят неудачу. [...] Если вовлечение сообщества не произойдёт, недоверие будет всегда. Это не паранойя, это просто реальность».[1256] Опасения по поводу влияния технологий алгоритмического полицейского контроля на сообщество не остались без внимания правоохранительных органов, с которыми были проведены интервью для этого отчёта. Например, старший констебль Райан Прокс из VPD заявил: «Я очень чувствителен к тому факту, что прогнозирующая полицейская деятельность рискует и в дальнейшем преследовать маргинализированные сообщества. Если мы собираемся пойти по этому пути и стать первым полицейским отделением в Канаде, чтобы сделать это, мы должны проявить должную осмотрительность. Это рискованное мероприятие, поскольку мы предприняли максимально активные шаги для предотвращения нарушений гражданских прав людей, насколько это возможно».[1257] Точно так же представитель SPPAL заявил: «Если технология, алгоритмы или какие-либо результаты не приводят к улучшению результатов для детей или людей, которые уязвимы, или делают сообщество более безопасным, то нет причин использовать какие-либо из этих технологий.[1258] Очевидно, что существует якобы консенсус среди представителей канадских правоохранительных органов, давших интервью для этого отчёта, в

[1255] See Section 5.3 («Rights to Freedom of Expression, Peaceful Assembly, and Association").
[1256] Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019).
[1257] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).
[1258] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

отношении нежелания подвергать исторически маргинализированные и уязвимые сообщества риску пострадать от алгоритмических полицейских технологий. При таком консенсусе полицейские службы должны осмысленно консультироваться с теми же сообществами и прислушиваться к ним до, во время и после внедрения любых таких технологий, особенно с группами, которые защищены разделом 15 Хартии и наиболее подвержены или затронуты алгоритмическим полицейским контролем.

5.4.3. Социально-экономические недостатки и гипервидимость для алгоритмической полицейской деятельности

Алгоритмическая дискриминация может происходить просто потому, что существует в обществе то, что делает человека более заметным для наблюдения со стороны правоохранительных органов и государственных и полицейских органов. Профессор Вирджиния Юбэнкс объясняет: «уязвимые группы сталкиваются с более высокими уровнями сбора данных, когда они получают доступ к общественным благам, проходят через тщательно охраняемые районы, входят в систему здравоохранения или пересекают национальные границы. Эти данные усиливают их маргинальность, когда используются, чтобы вызвать подозрения и дополнительное внимание».[1259] Помимо непосредственного беспокойства о конфиденциальности и свободе, [1260]такая повышенная «видимость данных» маргинализованных групп может сама по себе нарушать раздел 15.

Это явление увековечивает неблагоприятные условия для групп, защищённых разделом 15, подвергая их неравному и более безжалостному применению закона (через сотрудников полиции), одновременно ослабляя защиту закона, на которую они имеют право. В частности, такое неравное и несправедливое применение закона может нарушать их право на неприкосновенность частной жизни, право быть свободными от необоснованного обыска и изъятия, от произвольного задержания. Эти права защищены соответственно разделами 8 и 9 Хартии, а также законодательством о правах человека.

[1259] Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York: St. Martin's Press, 2018) at 7. Eubanks also points out that means-testing social welfare programs have «rationalized all manner of surveillance and policing of applicants and beneficiaries." Ibid at 28.

[1260] Полное обсуждение алгоритмической политики и права на неприкосновенность частной жизни см. в разделе 5.2 ("Право на неприкосновенность частной жизни"); анализ алгоритмического обеспечения соблюдения права на свободу и свободу от произвольного задержания см. в разделе 5.5 ("Право на свободу и свободу от произвольного задержания").

В своем глубоком анализе того, как алгоритмическое принятие решений вредит бедным людям, Юбэнкс связывает точки между исторически криминализованными бедняками и государством, использующим эту вменяемую преступность для оправдания инвазивных требований сбора данных в обмен на доступ к государственным услугам для удовлетворения базовых потребностей. Она пишет: «Такой общий доступ к глубоко личной информации не имеет смысла вне системы, которая приравнивает бедность и бездомность к преступности. Напротив, трудно себе представить тех, кто получает федеральные доллары за счёт налоговых вычетов по ипотеке или субсидируемых государством студенческих ссуд, подвергающихся такой тщательной проверке или имеющих доступ к их личной информации для правоохранительных органов без ордера. Более того, рост числа сборов, обмена и наблюдения за данными усиливает криминализацию бездомных хотя бы потому, что существует множество основных условий бездомности – негде спать, положить вещи,некуда пойти в туалет - тоже официально преступление.»[1261] «Криминализация бездомных» также имеет место по всей Канаде.[1262]Такая криминализация приводит к тому, что бездомные становятся более уязвимыми для вовлечения в систему уголовного правосудия, чем те, кто занимается незаконной деятельностью в стенах частных домов. Сара Брейн подробно останавливается на опасностях, которые возникают из-за этой формы алгоритмической предвзятости, когда она объясняет, что «ретроактивный характер полицейской деятельности в эпоху сбора данных с помощью драгнета означает, что информация регулярно накапливается, а файлы лежат в ожидании. В этом смысле, люди (бедные, бездомные или принадлежащие к расе) ведут инкриминирующую жизнь - повседневная деятельность, которая теперь кодируется в виде данных, может быть представлена в качестве доказательства постфактум».[1263] Брейн далее отмечает, что «непроверенные

[1261] Ibid at 116-117.

[1262] See e.g., Justin Douglas, «The Criminalization of Poverty: Montreal's Policy of Ticketing Homeless Youth for Municipal and Transportation By-Law Infractions" (2011) 16 Appeal 49; Damian Collins & Nicholas Blomley, «Private Needs and Public Space: Politics, Poverty, and Anti¬Panhandling By-Laws in Canadian Cities" in Law Commission of Canada, New Perspectives on the Public-Private Divide (Vancouver: UBC Press, 2003) at 56 <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.4772&rep=rep1&type=pdf#page=56>; Jackie Esmonde, «Criminalizing Poverty: The Criminal Law Power and the Safe Streets Act" (2002) Journal of Law and Social Policy 63; «The city where it's against the law to be poor", CBC Radio (4 January 2015) <https://www.cbc.ca/radio/thesundayedition/law-against-poverty-michael-s-essay-talking-to-terrorists- socks-for-the-homeless-documentary-1.2943464/the-city-where-it-s-against-the-law-to-be-poor-1.2943469>; and Stephen Gaetz, «The Criminalization of Homelessness: A Canadian Perspective" (2013) European Journal of Homelessness 357 <https://www.feantsa.org/download/ sg_response7772916537698278481.pdf>.

[1263] Sarah Brayne, «Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Review 977 at 1000-01. Эндрю Фергюсон также обсуждает опасности распознавания лиц, в частности, для тех, кто бездомный или иным образом вынужден проводить больше времени на улице: «[T] Настоящий прорывный сдвиг произойдет, когда технология распознавания лиц может быть использована для сопоставления людей на улице для оценки риска на компьютере. Хотя в настоящее время такой технологии распознавания лиц в реальном времени не существует - она ограничивается стационарными видеокамерами - технология разрабатывается для развертывания распознавания лиц на полицейских камерах и даже на нательных камерах полиции. В этом новом мире сочетания распознавания лиц из горячего списка будет означать, чтокаждый человек на улице может быть «пробит» и отслежен» . Andrew Guthrie Ferguson, «Illuminating Black Data Policing" (2018) 15 Ohio

прогнозы ... могут оправдывать чрезмерную политику меньшинства и потенциально отнимают ресурсы у людей и территорий, невидимых для датчиков сбора данных или подлежащих систематическому занижению».[1264]

Одна из самых больших уловок, связанных со всей алгоритмической и предсказательной полицейской технологией, заключается в том, что раскрытие преступлений бедных только кажется полезным. Нет отчета меньшинства, так сказать, для богатых. – Десмонд Коул (писатель, журналист и активист расовой справедливости)[1265]

То, что обсуждают Юбэнкс и Брейн, является формой поговорки «то, что измеряется, управляется»: потому что те, кто живёт около черты бедности или ниже неё, а также маргинализированные в других отношениях люди, чаще подвергаются своего рода измерению посредством государственного мониторинга, количественной оценки и, если сводиться к грубым данным, они систематически становятся более восприимчивыми к так называемому управлению - и неправильному управлению - со стороны правоохранительных органов, в отличие от более привилегированных членов общества.[1266]Проблема алгоритмических полицейских технологий в этом контексте заключается в том, что они в подавляющем большинстве сосредоточены на определённых типах преступлений и правонарушителей (например, преступлениях против собственности на улицах или бандитских преступлениях), пренебрегая обучением того же алгоритмического взгляда на другие виды преступлений и правонарушителей (например, экологические преступления или уголовные

State Journal of Criminal Law 503 at 521 (footnotes omitted).

[1264] Sarah Brayne, «Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Review 977 at 998 (сноски опущены). Заявление Брейна обращает внимание на ошибочность того, что система может что-то измерить система, не говоря уже о лучшей метрике, по которой можно оценить результаты, когда это может быть не так. См. также Кэти О 'Нил, «Оружие уничтожения математики»: как большие данные увеличивают неравенство и угрожают демократии (Нью-Йорк: Crown Publishing Group, 2016). На самом деле такие показатели, возможно, просто были наиболее легко измеримыми и, таким образом, неправильно рассматривались как наиболее важные показатели эффективного правоприменения или общественной безопасности. Насколько известно авторам, не было проведено исследований, в ходе которых было установлено, что сосредоточение внимания исключительно на разработке методов прогнозирования уличных преступлений приведет к повышению общей общественной безопасности и благосостояния по сравнению с сосредоточением внимания на предотвращении некоторых других видов преступлений с тем же объемом ресурсов.

[1265] Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

[1266] В другом примере высказывания эмпирические исследования, проведенные шотландцем Уортли и другими исследователями, указывают на расизм и расовое профилирование со стороны полицейских служб в качестве явления, подлежащего измерению, и, таким образом, в большей степени рассматриваются как "управляемые" или рассматриваемые в качестве серьезной проблемы государственной политики, связанной с системой правосудия. See e.g., Scot Wortley, «Police Use of Force in Ontario: An Examination of Data from the Special Investigations Unit: Final Report" (Research Project Conducted on behalf of the African Canadian Legal Clinic for Submission to the Ipperwash Inquiry) <https://www.ttorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/projects/pdf/AfricanCanadianClinicIpperwashProject_SIUStudybyScotWortley. pdf>; Scot Wortley & Akwasi Owusu-Bempah, «The usual suspects: police stop and search practices in Canada" (2011) 21:4 Policing and Society 395; Steven Hayle, Scot Wortley, & Julian Tanner, «Race, Street Life, and Policing: Implications for Racial Profiling" (2016) 58:3 Canadian Journal of Criminology and Criminal Justice 322.

преследования). Чтобы быть ясным, это не означает, что алгоритмическое наблюдение должно быть расширено для включения более широкого круга преступлений, учитывая соображения конфиденциальности, изложенные в разделе 5.2 («Право на конфедициальность»). Скорее, эти тенденции представляют собой ещё одну форму неравенства, связанного с алгоритмической политикой в отношении маргинализированных групп.

В частности, избирательность фокуса может представлять собой форму дискриминации с неблагоприятными последствиями в соответствии с разделом 15 при использовании алгоритмической полицейской технологии для определенных видов преступлений. Непропорционально большое внимание уделяется членам сообществ, которые определены охраняемыми территориями (вместо того, чтобы использовать грозный государственный аппарат наблюдения на предполагаемых подозреваемых и потенциальных преступниках с социально-политическими и социально-экономическими преимуществами).[1267] Кроме того, неблагоприятное социально-экономическое положение переплетается с историческим и постоянным системным неблагоприятным положением на основе других защищенных оснований и часто является прямым результатом его передачи из поколения в поколение.[1268] Следовательно, необходимо принимать во внимание бедность, бездомность и социально-экономический статус, прежде чем внедрять какие-либо новые технологии, где на карту поставлена уголовная опасность. Присутствие и действия маргинализированных лиц могут быть просто более заметны для алгоритмической полицейской технологии и связанных с ней инструментов правоохранительных органов, которые предназначены для обнаружения признаков преступности. Однако, сама по себе видимость ничего не говорит о фактической преступности. Тем не менее, это непропорциональное воздействие на то, что их видит, исследует и обрабатывает система уголовного правосудия, сопряжено с особенно высокими ставками для сообществ, которые уже подвергаются чрезмерному контролю и несправедливо чрезмерно представлены на последующих этапах системы. Например, чернокожий или

[1267] For a satirical and pointed proof-of-concept, see Brian Clifton, Sam Lavigne, & Francis Tseng, «Predicting Financial Crime: Augmenting the Predictive Policing Arsenal", The New Inquiry (2017) <https://arxiv.org/pdf/1704.07826.pdf>; «White Collar Crime Risk Zones", Brian Clifton, Sam Lavigne, & Francis Tseng, «White Collar Crime Risk Zones", The New Inquiry <https://whitecollar.thenewinquiry.com>; and Katharine Schwab, «Proof That Algorithms Pick Up Our Biases, In A Single Map", Fast Company (26 April 2017) <https://www.fastcompany.com/90111752/proof-that-algorithms-pick-up-our-biases-in-a-single-map>.

[1268] See e.g., Bourassa et al, «Understanding the Intergenerational Effects of Colonization: Aboriginal Women with Neurological Conditions — Their Reality and Resilience" (2015) 10:2 International Journal of Indigenous Health (revised references 2016) 3 at 9-11; Savannah Hope et al, «Intergenerational Trauma and Aboriginal Homelessness" (September 2017), online (pdf): Social Planning and Research Council of Hamilton <http://www.sprc.hamilton.on.ca/wp-content/uploads/2017/09/Intergenerational_Trauma_and_Aboriginal_Homelessness_2017.pdf>; Valerie J Pruegger, Derek Cook & Sybille Richter-Salomons, «Inequality in Calgary: The Racialization of Poverty" (2009), online (pdf): City of Calgary <https://www.calgary.ca/csps/cns/publications-guides-and-directories/inequality-in-calgary.html>; and Paul J Kim, «Social Determinants of Health Inequities in Indigenous Canadians Through a Life Course Approach to Colonialism and the Residential School System" (2019) 3:1 Health Equity 378.

коренной житель с самого начала подвергается более высокому риску наблюдения и подозрений, а после наблюдения подвергается более высокому риску быть подвергнутым обыску или задержанию и аресту. После задержания они подвергаются более высокому риску ненужного применения силы. После ареста им грозит повышенный риск предъявления обвинения. После предъявления обвинения они подвергаются более высокому риску заключения в тюрьму с более суровыми условиями и на более длительные сроки по сравнению с белыми людьми. И, наконец, попав в тюрьму, они подвергаются более высокому риску подвергнуться более жестокому обращению по сравнению с белыми людьми при тех же или подобных обстоятельствах. Следовательно, первые встречи с правоохранительными органами, которые могут рассматриваться членами групп (таких как богатые или политически влиятельные), которые исторически поддерживали хорошие отношения с учреждениями уголовного правосудия, «невысокие ставки», «могут привести к более серьёзным вмешательствам полиции» в случае исторически чрезмерно перегруженных групп.[1269] Каждое столкновение рискует нарушить право маргинализованного человека на свободу и равенство, право на свободу от дискриминации и право на свободу от необоснованного обыска и конфискации. Любое из этих начальных нарушений может легко превратиться в несколько слоёв последующих злоупотреблений и несправедливого обращения на каждом последующем этапе системы уголовного правосудия, даже если пострадавшее лицо не сделало ничего, что требовало бы тщательной проверки.

Чистота или неправомерное поведение на основе расового профилирования, предвзятого набора данных, плохо разработанного алгоритма или всего вышеперечисленного могут привести к алгоритмически изменённым судьбам с серьёзными и далеко идущими последствиями для маргинализированных лиц и сообществ, которые защищены в соответствии с разделом 15 Хартии.

[1269] Ontario Human Rights Commission, Under Suspicion: Research and consultation report on racial profiling in Ontario (April 2017), at 38 <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario>.

В фокусе внимания № 6

Эволюционирующий закон о социально-экономическом статусе как защищаемом правозащитном основании равенства и свободы от дискриминации

Конституционность дискриминации по признаку социально-экономического статуса с низким доходом – это постоянно развивающаяся проблема в Канаде. Канадские суды пока в целом не признают бедность или социально-экономический статус как подпадающие под аналогичное основание в соответствии с разделом 15. Учёные-правоведы призвали признать бедность в качестве определяющей характеристики, которая даёт основание для защиты в соответствии с разделом 15 Хартии.[1270] Решения начали вырисовывать контуры возникающего признания связи между социально-экономическим статусом и дискриминацией. Полное признание этой связи обеспечило бы людям, не имеющим социально-экономического статуса, равный доступ к правам в соответствии с Хартией в Канаде[1271]

Например, в решении 2018 года по делу R v Meads,[1272] Апелляционный суд Онтарио отменил закон, который отказывал лицам в повышении кредита на содержание под стражей до суда на том основании, что они не смогли указать причину, по которой они не должны содержаться под стражей до суда (поскольку против освобождения под залог). Суд постановил, что одна из причин нарушения раздела 7 Хартии заключалась в том, что состоятельные люди с большей вероятностью продемонстрируют, почему они должны вносить залог. Этот анализ важен в контексте инструментов прогнозирования, поскольку возможность внести залог - это, по сути, вопрос о риске (или его отсутствии) и, таким образом, аналогичен инструменту прогнозирования. Аргументация суда имеет значение для анализа равноправия в алгоритмической полицейской деятельности, поскольку суд заявил, что непропорционально невыгодное положение обвиняемых, являющихся неимущими, нарушает Хартию. Решение по делу Мидса было принято в соответствии со статьей 7 (закон был чрезмерно широким), но он имеет отношение к разделу 15, поскольку закон был чрезмерно широким и основывался на принципах равенства и свободы от дискриминации. Суд установил, что «бедные и

[1270] See e.g., the history tracing jurisprudence of an «effort to disappear the poor within section 15(1)" in Kerri Froc, «Immutability Hauntings: Socioeconomic Status and Women's Right to Just Conditions of Work under Section 15 of the Charter" in Martha Jackman and Bruce Porter, eds, Advancing Social Rights in Canada (Toronto: Irwin Law, 2014) 187.

[1271] Boudreault, 2018 SCC 58; Quebec (Attorney General) v Alliance du personnel professionnel et technique de la sante et des services sociaux, 2018 SCC 17; and R v Le, 2019 SCC 34 at para 59.

[1272] R v Meads, 2018 ONCA 146.

социально изолированные лица» из-за бедности, психического здоровья или зависимости не будут иметь доступа к ресурсам, необходимым для доказательства того, что они соответствуют критериям досудебного освобождения. Таким образом, задержание будет результатом «неблагоприятного социального и экономического положения», а не какого-либо проступка. Таким образом, закон не имел «рациональной связи с целью предотвращения неправомерных действий при освобождении». [1273] Примеры актуальности бедности как аналогичного основания появляются в решениях судов и трибуналов низшей инстанции, которые признали более узкие родственные характеристики, такие как государственное жилье. Эволюционирующий закон о социально-экономическом статусе как защищённом основании прав человека, равенства и свободы от расовой дискриминации, одиноких матерей или женщины-иммигрантов; и матерей-одиночек, получающих социальное пособие – в качестве аналогичного основания.[1274] Провинциальные законы о правах человека в Квебеке, [1275] Нью-Брансуике и Северо-Западных территориях также признают «дискриминацию в отношении лиц, находящихся в неблагоприятном социальном и экономическом положении, таких как получатели социальной помощи и работники в нестандартных условиях, замещающие низкооплачиваемые должности, которые сталкиваются с дискриминационными предположениями относительно, например, их способности платить за аренду, товары и услуги. [1276]

В контексте уголовного правосудия дело «Р. против Ле» является знаковым делом о конституционной свободе и неприкосновенности частной жизни с участием расовых лиц, и социально-экономически неблагополучных слоев населения. В этом решении Верховный суд Канады установил, что «мы подошли к тому месту, где исследование показывает непропорциональную

[1273] Ibid at para 46.

[1274] Sparks v Dartmouth/Halifax (County) Regional Housing Authority, 119 NSR (2d) 91 (NSCA); Kearney v Bramalea Ltd. (No. 2) (1998), 34 CHRR D/1 (Ont Bd Inq); and Falkiner et al v Ontario (Director of Income Maintenance, Ministry of Community & Social Services) (2002), 159 OAC 135 (CA).

[1275] «По мнению Комиссии, социальное профилирование является одной из форм дискриминации в соответствии со статьей 10 Квебекской хартии прав и свобод человека... включая "социальное условие". Социальное состояние является запрещенным основанием для дискриминации в соответствии с Квебекской хартией с момента ее принятия в 1975 году.... Бездомность признается судами по правам человека, судами и Комиссией Квебека по правам человека в качестве одной из форм "социального положения". Marie-Eve Sylvestre and Celine Bellot, «Challenging Discriminatory and Punitive Responses to Homelessness in Canada" in Martha Jackman and Bruce Porter, eds, Advancing Social Rights in Canada (Toronto: Irwin Law, 2014) 155 at 172-73.

[1276] «Квебек и Нью-Брансуик также принимают объективно-субъективный критерий социального состояния в руководящих принципах своих соответствующих комиссий по правам человека... С течением времени в Квебеке этот критерий развивался в целях борьбы с дискриминацией в отношении лиц, страдающих от социально-экономического неблагополучия, таких, как получатели социальной помощи и работники, занятые на нестабильных и низкооплачиваемых должностях, которые сталкиваются с дискриминационными предположениями, касающимися, например, их способности оплачивать аренду или товары и услуги." Wayne MacKay & Natasha Kim, «Adding Social Condition to the Canadian Human Rights Act", Canadian Human Rights Commission (February 2009) at 3 <http://publications.gc.ca/collections/collection_2012/ ccdp-chrc/HR4-14-2009

работу полиции над расовыми и низкодоходными сообществами». [1277]Такое развитие юриспруденции по вопросам равенства будет иметь последствия для будущего прецедентного права и, таким образом, необходимо контролировать, учитывая растущее признание того, что бедность сама по себе долгое время была причиной противоправной дискриминации.

5.4.4. Неравенство по замыслу и несправедливость

Дискриминация неблагоприятных эффектов в алгоритмической реализации политик может быть результатом того, как разработан алгоритм.[1278]Программисты делают ряд важных решений при разработке кода, который будет использоваться для уголовного правосудия. Этот выбор может быть отягощён ранее существовавшими предубеждениями, оценочными суждениями, отсутствием специальных знаний или жизненного опыта, или незнанием реальных последствий определённых математических решений для маргинализированных лиц и их сообществ. Например, компания Equivant (ранее Northpointe) разработала алгоритм прогнозирования рецидивов, профилирование исправительных правонарушителей для альтернативных санкций (COMPAS) в соответствии с определенным пониманием того, что, по их мнению, означает справедливость алгоритма.[1279] И все же COMPAS закрепил кодексом предвзятость против чернокожих подсудимых, закрепив неравенство умышленно. По словам компьютерного учёного Арвинда Нараянана, существует как минимум 21 различное определение справедливости, которые можно использовать при разработке алгоритма, каждое из которых продвигает одни ценности и политику по сравнению с другими.[1280]Тем, кто разрабатывает алгоритм, такой как COMPAS, возможно, придётся выбрать (или они могут неосознанно решить) между, например, установлением приоритета равной точности прогнозов для всех групп, минимизацией ложных отрицательных результатов перед минимизацией

[1277] R v Le, 2019 SCC 34 at para 97.

[1278] «Учитывая гибкий и податливый способ, которым алгоритмы ML [машинного обучения] обучаются и развиваются, обучение алгоритму может быть сопряжено с опасностями в отношении характеристики и взвешивания входных данных". Royal United Services Institute, Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges (September 2018) at 24-25 <https://rusi.org/sites/default/files/201809_ whr_3-18_machine_learning_algorithms.pdf.pdf>.

[1279] В частности, Northpointe откалибровал алгоритм так, чтобы он имел одинаковую прогностическую точность как для белых, так и для черных ответчиков по всей доске, но это привело к тому, что алгоритм имел более высокую ложноположительную частоту для черных ответчиков и более высокую ложноотрицательную частоту для белых ответчиков. Matthias Spielkamp, «Inspecting Algorithms for Bias", MIT Technology Review (12 June 2017) <https://www. technologyreview.com/s/607955/inspecting-algorithms-for-bias/>.

[1280] Arvind Narayanan, «Tutorial: 21 fairness definitions and their politics" (1 March 2018), YouTube <https://www.youtube.com/ watch?v=jIXIuYdnyyk>; Arvind Narayanan, «Tutorial: 21 fairness definitions and their politics" (23 February 2018), Google Docs <https://docs. google.com/document/d/1bnQKzFAzCTcBcNvW5tsPuSDje8WWWY-SSF4wQm6TLvQ/edit>.

ложных срабатываний,[1281] или приоритезация максимизации истинных положительных результатов за счёт увеличения количества ложных срабатываний. Многие варианты дизайна так или иначе связаны с компромиссом, но те, на кого больше всего влияют полицейские алгоритмы - например, лица, попавшие в систему уголовного правосудия или неправомерно привлечённые к уголовной ответственности правоохранительными органами, полагающимися на алгоритмические оценки, - имеют мало скажите, в чем заключаются компромиссы.

Алгоритмы, которые используются для полицейских и правоохранительных целей и которые намеренно создают невыгодное положение для лиц в защищённой группе, будут или должны считаться нарушением раздела 15. В деле Эверт против Канады, например, оспариваемые инструменты оценки рисков были спроектированы, разработаны, протестированы и утверждены без учёта ответчиков из числа коренных народов и без их участия, даже несмотря на то, что эти инструменты сейчас используются. Верховный суд Канады не обнаружил, что использование этих инструментов Службой исправительных учреждений Канады нарушает права г-на Эверта, указанные в разделе 15, на том основании, что не было достаточных доказательств того, что эти инструменты «на самом деле переоценивают риск, создаваемый сокамерниками из числа коренного населения, или привести к более суровым условиям содержания или к отказу в реабилитационных возможностях из-за такой завышенной оценки».[1282]

Этот вывод предполагает, что при наличии доказательств такой переоценки, более суровых последствий или отказа в льготах для защищённой группы - как в случае с COMPAS - суд может решить, что использование такого инструмента действительно нарушает раздел 15.

Технологии алгоритмической полицейской деятельности могут не только кодировать неравенство и дискриминацию в системе уголовного правосудия, но они также маскируют эту несправедливость в силу своей зависимости от алгоритмов. Принятие этих инструментов может придать системам алгоритмического контроля вид научной и математической «непогрешимости», «нейтральности» или «объективности». Этот феномен одновременно скрывает коренные причины неравенства и связанной с ним социально-политической несправедливости, алгоритмы которых выдвигаются для якобы «решения», отвлекая время, внимание и ресурсы от подлинных реформ, лежащих в основе

[1281] Hannah Couchman, «Policing by Machine: Predictive policing and the threat to our rights," (January 2019) Liberty, at 50-51<https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.

[1282] Ewert v Canada, 2018 SCC 30 at para 79.

структурных или институциональных систем и моделей ущерба.[1283] По словам Рухи Бенджамина алгоритмические пластыри для лечения глубоко укоренившихся социальных недугов «предлагают прагматическое включение вместо политических и социальных преобразований. [...] Исправления в новом коде Джима – постоянный заменитель для более смелых изменений».[1284] В качестве примера Коалиция Stop LAPD Spying Coalition указывает на системный расизм как на основную проблему, которую должны решать правоохранительные органы, правительства и общество в целом. Вместо того, чтобы пытаться улучшить алгоритмическую деятельность полиции, «критические расовые теоретики утверждают, что ... полное уничтожение расизма в одном контексте требует одновременного рассмотрения других форм угнетения в других контекстах ... Иными словами, проблемы, связанные с неравенством в системе уголовного правосудия, существовали до и за пределами алгоритмов; их решения выходят за рамки компетенции и ограничений алгоритмов.

5.4.5. Заключительные комментарии: алгоритмическая деятельность полиции и право на равенство и свободу от дискриминации

Проблемы равенства и дискриминации лежат в основе многих проблем, связанных с технологиями алгоритмической полицейской деятельности. Такие технологии объединяют две области, которые исторически дискриминировали группы, защищённые разделом 15: уголовное правосудие и алгоритмическое принятие решений (как подмножество технологического сектора в более широком смысле). В дополнение к конкретным вопросам равенства, рассмотренным выше, два дополнительных пересекающихся соображения являются ключевыми для оценки алгоритмических технологий полицейского контроля в отношении прав по разделу 15. Во-первых, нарушения раздела 15, которые могут происходить в результате алгоритмического контроля, могут непропорционально ущемить другие права маргинализированных лиц, такие как право на неприкосновенность частной жизни и свободу от необоснованного обыска и конфискации,[1285]право на свободу и свободу от произвольного задержания,[1286] право на презумпцию невиновности.[1287]Таким образом, когда

[1283] ADS [автоматизированные системы принятия решений] часто принимаются для того, чтобы избежать или запутать более широкие структурные и системные проблемы в обществе - проблемы, которые часто выходят за рамки возможностей учреждений с ограниченными денежными средствами для значимого решения ". Meredith Whittaker et al, «AI Now Report 2018" (December 2018), AI Now Institute, at 40 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

[1284] Ruha Benjamin, Race After Technology: Abolitionist Tools for the New Jim Code (Cambridge: Polity Press, 2019) at 156-57.

[1285] See Section 5.2 («Right to Privacy").

[1286] See Section 5.5 («Right to Liberty and to Be Free from Arbitrary Detention").

государство взаимодействует, использует или полагается на технологии алгоритмического контроля за особым ущербом для маргинализированных сообществ, например, сбор данных частного сектора от коммерческих организаций, получение данных от агентств социальных услуг, которые в первую очередь обслуживают маргинализованные сообщества, с использованием данных – методы выявления лиц на основе защищённых характеристик или более частые остановки полиции в отношении маргинализированных лиц или внутри их сообществ на основе алгоритмических показателей – государство может нарушать свои внутренние и международные обязательства в области прав человека по поддержанию равенства и свободы от дискриминации. Во-вторых, учитывая непрозрачный и часто приватизированный характер алгоритмической полицейской технологии, глубоко укоренившуюся распространённость системной дискриминации и исторические трудности с доказательством неблагоприятных последствий дискриминации в суде,[1288] следует рассмотреть возможность реализации обратного бремени в утверждениях раздела 15, касающихся алгоритмической предвзятости. Тереза Скасса указала, что в деле Эверт против Канады потребовалось «[ответчику] 18 лет [и] преданной команде юристов»[1289] для продвижения судебного процесса. Она предположила, что требование «продемонстрировать дискриминационные воздействия или эффекты или показать, как сам алгоритм и/или данные, использованные для его разработки, включают предвзятость или дискриминационные предположения [...], налагают значительное бремя доказывания»[1290] о будущих партиях, которые, вероятно, будут уже маргинализованными людьми. Ученые-юристы также ранее предлагали реализовать обратное бремя в контексте расового профилирования и произвольного задержания в соответствии с разделом 9 Хартии на основе аналогичных соображений справедливости.[1291]

[1287] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 11(d).

[1288] «До настоящего времени лишь немногие решения Верховного суда касались дискриминации в связи с негативными последствиями, возможно, из-за значительных практических трудностей, связанных с представлением достаточных доказательств для демонстрации негативных последствий для конкретных групп, таких, как женщины (Саймс против Канады, [1993] 4 S.C.R. 695). В тех случаях, когда в соответствии с Хартией иски о негативных последствиях были удовлетворены, они основывались на самоочевидных общественных моделях, поддающихся судебному уведомлению.... "«Section 15 - Equality rights", Department of Justice (17 June 2019) <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ ccrf-ccdl/check/art15.html>.

[1289] Teresa Scassa, «Supreme Court of Canada Decision Has Relevance for Addressing Bias in Algorithmic Decision-Making", Teresa Scassa (14 June 2018) <www.teresascassa.ca/index.php?option=com_k2&view=item&id=278:supreme-court-of-canada-decision-has-relevance-for- addressing-bias-in-algorithmic-decision-making&Itemid=80>.

[1290] Ibid.

[1291] См., например, "В свете этих свидетельств [расового профилирования чернокожих водителей] и свидетельств системного расизма в Канаде бремя доказывания, предусмотренное в разделе 9, должно переложиться на Корону, с тем чтобы на основе баланса вероятностей установить, что так называемая обычная остановка автомобиля чернокожего водителя не была мотивирована расовой принадлежностью. [...] Это бремя согласуется не только с принципами равенства и справедливости, но и с прецедентами и политикой. [...] Поскольку полиция является частью системы отправления правосудия, Корона должна нести ответственность

Снятие этого бремени позволило бы признать огромные проблемы, с которыми сталкиваются стремящиеся к равенству маргинализированные люди, которые пытаются доказать, что технология алгоритмической полицейской деятельности является дискриминационной. Отсутствие у таких лиц доступа к данному алгоритму в сочетании с другими областями явной асимметрии информации почти несомненно поставит государственных субъектов и частный сектор в лучшие возможности для предоставления соответствующих доказательств почти в каждом случае. И наконец, несколько рекомендаций по политике вытекают из анализа предвзятости в дизайне, данных, контроле и влиянии на сообщество в контексте технологии алгоритмического контроля. Эти рекомендации снизят риски или последствия нарушений раздела 15, связанных с такой технологией, и должны начинаться с обеспечения того, чтобы исторические наборы полицейских данных не использовались для обучения или работы правоохранительных алгоритмов. Предотвращение и смягчение последствий нарушений раздела 15 также требует значимого участия и консультаций с маргинализованными и исторически чрезмерно криминализованными сообществами, которые должны быть интегрированы в любой процесс проектирования, разработки или внедрения технологии алгоритмического контроля. Хотя обучение сотрудников полиции играет важную роль для смягчения неосознанной предвзятости и предвзятости автоматизации, когда их отправляют в алгоритмические «горячие точки» или где они взаимодействуют со «списком участников» или лицами, прошедшими алгоритмическую оценку риска. Исследования показали, что такое обучение часто проводится не эффективно и, следовательно, не может противостоять существенным причинам для запрета или строгого ограничения использования алгоритмических полицейских технологий там, где они создают риски для равенства и свободы от дискриминации. Дальнейшие меры по предотвращению или смягчению последствий включают отслеживание выходных данных алгоритмов полицейской деятельности на постоянной основе для отслеживания проблемных тенденций, которые, нацелены на маргинализированные сообщества или демонстрируют предвзятость в отношении групп, защищённых разделом 15; установка брандмауэра для предотвращения или минимизации обмена данными между поставщиками социальных услуг и правоохранительными органами; и пересмотр того, действительно ли технология алгоритмического контроля является подходящим решением, в

за такие проступки полиции, как расовое профилирование. " David M Tanovich, «Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention" (2002) 40:2 Osgoode Hall Law Journal 145 at 181-82. Regarding the establishing of investigative detention in R v Mann, 2004 SCC 52: «[G]iven the evidence of amenability to abuse, the odd fit between investigative detentions and ss. 10(a-c) of the Charter, and the novel nature of the power, had it been alive to the racial aspect of this issue, the Supreme Court might have held that the Crown should bear the burden of showing that an investigative detention is reasonable and justified." Benjamin L Berger, «Race and Erasure in R. v. Mann» (2004) 21 Criminal Reports (Articles) 58 (WL). See also Gabriella Jamieson, «Using Section 24(1) Charter Damages to Remedy Racial Discrimination in the Criminal Justice System" (2017) 22 Appeal 71 at 85-86 («A Shifting Burden in the Future?").

отличие от направления ресурсов и внимания на лежащие в основе существенные социальные проблемы и коренные причины, такие как системный расизм или классизм.

5.2 Право на свободу и свободу от произвольного задержания

Конституционное право Канады и международное право в области прав человека гарантируют право на жизнь, свободу и безопасность человека, включая право не подвергаться произвольному задержанию. Всеобщая декларация прав человека и ICCPR устанавливают «право на свободу и личную неприкосновенность», а также право не подвергаться «произвольному аресту или задержанию».[1292]

Аналогичным образом, раздел 9 Канадской хартии предоставляет каждому человеку «право не подвергаться произвольному задержанию или тюремному заключению», а раздел 7 гарантирует, что каждый «имеет право на жизнь, свободу и личную безопасность, а также право не быть лишенным свободы, кроме как в соответствии с принципами фундаментальной справедливости».[1293]

Технологии алгоритмической полицейской деятельности задействуют права свободы, указанные в разделах 9 и 7, поскольку они увеличивают риск того, что человек может быть арестован или задержан произвольно, или лишён свободы способом, который не соответствует принципам фундаментальной справедливости. В следующих подразделах этого отчёта анализируются две основные проблемы, связанные с технологиями алгоритмического контроля в этом отношении. Раздел 5.5.1 демонстрирует, как использование алгоритмической полицейской технологии для ареста или задержания человека может не соответствовать стандарту «разумного подозрения» или «разумных оснований» в канадском законодательстве. Опора на алгоритмические прогнозы не соответствует требуемому стандарту, потому что алгоритмические прогнозы включают обобщенные прогнозы, которые могут привести к генерализованным подозрениям, заменяющим индивидуальные оценки чьих-либо личных характеристик и поведения, что потенциально делает арест или задержание неконституционными. В разделе 5.5.2 обсуждается проблема

[1292] The UDHR states, «Everyone has the right to life, liberty and security of the person" and «No one shall be subjected to arbitrary arrest, detention or exile:" Universal Declaration of Human Rights, adopted December 10, 1948, GA Res 217A(III), UN Doc A/810 at 71 (1948), arts 3 and 9. Article 9 of the ICCPR states, «Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law."

[1293] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, ss 7 and 9.

неосознанной предвзятости среди сотрудников правоохранительных органов и других субъектов системы уголовного правосудия, особенно проявляющейся в расовой предвзятости и расовом профилировании. Технологии алгоритмической полицейской деятельности могут способствовать усилению расового профилирования, которое, как установили канадские суды, делает задержание или арест произвольным и, следовательно, неконституционным.

Из-за некоторого совпадения тематики правовой и политический анализы в этом разделе будут сосредоточены в разделе 9, а вопросы раздела 7 будут обсуждаться позже в разделе 5.6 («Право на надлежащую правовую процедуру»).

5.5.1. Алгоритмический контроль и общие подозрения

В канадском уголовном и конституционном праве стандарт разумного подозрения – это то, что не позволяет задержанию быть произвольным и, следовательно, неконституционным. Стандарт «предотвращает неизбирательное и дискриминационное использование полицейских полномочий».[1294] Алгоритмический контроль может угрожать праву на свободу от произвольного задержания на основании того, как алгоритмические прогнозы могут взаимодействовать с подозрениями полицейских на практике, и как эти прогнозы могут повлиять на правовой анализ для обоснованного подозрения в законе.[1295]

Для того чтобы подозрение было «обоснованным», согласно разделу 9 судебной практики, подозрение должно быть связано с характеристиками и поведением человека. Основания для задержания должны быть разумными и объективно установленными.[1296]

Выявление обоснованного подозрения включает в себя оценку «совокупности обстоятельств, основанных на объективно различимых фактах, которые подлежат независимой и строгой судебной проверке».[1297] Таким образом, основания для задержания не могут быть сформированы на основе недостоверной информации, такой как неверные или неточные данные, или на основе предвзятых или дискриминационных выводов. Таким образом, использование алгоритмических прогнозов для оправдания лишения свободы (например, следственного задержания на улице) вызывает озабоченность в

[1294] R v Mann, [2004] 3 SCR 59; R v Chehil, 2013 SCC 49 at para 3.
[1295] See generally Andrew Guthrie Ferguson, «Predictive Policing and Reasonable Suspicion" (2013) 62:2 Emory Law Journal 259 at 309-310.
[1296] R v Chehil, 2013 SCC 49.
[1297] Ibid at para 3.

связи с разделом 9, если полицейская служба не установила надежность алгоритма или лежащих в его основе данных.

Алгоритмические методы контроля, как правило, по определению полагаются на обобщенные выводы. Таким образом, эти методы противоречат установленному закону, согласно которому разумные подозрения не могут основываться на общих подозрениях, [1298]например, подозрение, основанное на убеждениях об этнической группе или месте, где был обнаружен человек. Использование алгоритмических полицейских технологий в качестве основания для подозрений может нарушить раздел 9, в котором алгоритмические прогнозы основаны на статистических тенденциях, а не на конкретном человеке.

Офицеры могут подсознательно полагаться на прогноз риска, созданный алгоритмом, чтобы сформировать основания для подозрений, которые они считают «разумными», даже если «действия [подозреваемого или задержанного лица] вообще не изменились. Объективно, что подозреваемое лицо является не более или менее подозрительным, или преступным, чем лицо, которое не подвергалось прогнозированию повышенного риска. Тем не менее, на этот прогноз в сочетании с профилем общей преступной деятельности» офицер может полагаться, чтобы сформулировать подозрения или оправдать задержание - даже если не было других оснований для подозрений из-за отсутствия алгоритмического инструмента. [1299]Таким образом, алгоритмические прогнозы могут приводить к задержаниям, основанным на общих подозрениях или сомнительной надёжности алгоритма или лежащих в его основе данных. Результатом является потенциальное увеличение количества неконституционных задержаний (включая остановки полиции), чем это могло бы произойти в отсутствие алгоритмических технологий полицейского надзора.

Исследования в этой области широко признали проблему «предвзятости автоматизации», определяемой как склонность людей «полагаться на суждения об автоматизированных решениях как на превосходящие их собственные, даже если у них есть основания полагать, что технология несовершенна».[1300] Признавая эти опасения в интервью для этого отчёта, старший констебль Райан Прокс из VPD ответил, что офицеров специально учат не полагаться на алгоритмические прогнозы как на основание для подозрений. [1301]Однако ни

[1298] R v Kang-Brown, 2008 SCC 18.

[1299] Andrew Guthrie Ferguson, «Predictive Policing and Reasonable Suspicion" (2013) 62:2 Emory Law Journal 259.

[1300] Lindsey Barrett, «Reasonably Suspicious Algorithms: Predictive Policing at the United States Border" (2017) 41 NYU Review of Law & Social Change 327 at 342-43 <https://socialchangenyu.com/wp-content/uploads/2017/09/barrett_digital_9-6-17.pdf>.

[1301] Прокс заявил: "С точки зрения обучения мы четко даем понять, что если сотрудники полиции развернуты в прогнозируемых местах, вы не можете использовать систему прогнозирования в качестве основания для проверки улиц. [...] Только потому, что вы видите, что кто-то идет по улице, прогноз не дает вам права на

интервью, ни исследование для этого отчёта не выявили официальных письменных правил, которые усилили бы это обучение.

Кроме того, одной только подготовки, вероятно, недостаточно, чтобы устранить риск предвзятого отношения к автоматизации среди офицеров.[1302] Более того, обучение является лишь одним из компонентов более широкой полицейской культуры и практики, а VPD – лишь одна из более чем 140 муниципальных полицейских служб Канады.[1303]Без эффективного обучения, технологической грамотности, культурной компетентности и соответствующих передовых методов во всех правоохранительных органах страны люди по-прежнему будут подвергаться повышенному риску нарушения их прав, предусмотренных разделом 9, из-за предвзятости автоматизации и других предубеждений в алгоритмической работе полиции. Ясные письменные политики, директивы и значимые механизмы подотчётности рекомендуются и обсуждаются далее в части 6 («Рекомендации и заключение») настоящего отчета.

5.5.2. Бессознательное предубеждение и расовое профилирование

Технологии алгоритмического контроля очень чувствительны к включению и закреплению неосознанных предубеждений их разработчиков, отражению предубеждений, заложенных в их обучающих данных, и усугублению любых неосознанных предубеждений у людей, использующих такие технологии. Их высказывания о подозрительных людях или местах могут увековечить предвзятость. Факторы, вызывающие разумные подозрения, «должны соответствовать принципам Устава и должны относиться к действиям объекта расследования, а не к его или её неизменным характеристикам».[1304] Таким образом, использование алгоритмических инструментов может создать серьезные конституционные проблемы и проблемы с правами человека, когда алгоритм генерирует прогнозы на основе неизменных характеристик человека

проверку улицы. Все равно нужно формировать свои основания для участия в любом качестве с представителем общественности ". Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

[1302] Смотрите, например, "Другие исследования, цитируемые авторами, хотя и в контексте смещения автоматизации, показывают, что даже явные брифинги о факторах риска в HCI [взаимодействие человека с компьютером] не смягчают силу смещения автоматизации, и это, по-видимому, верно как в многозадачной, так и в одиночной среде. Холостой разум - это не пустой разум, а скорее блуждающий разум, и когда ставки высоки, риск самоуспокоения все еще слишком велик, чтобы им можно было управлять с помощью тренировочных вмешательств с резиновыми штампами, которые делают только сомнительную разницу в глубоких психологических ценностях". John Zerilli, Alistair Knott, James Maclaurin & Colin Gavaghan, «Algorithmic Decision-Making and the Control Problem" (2019) 29 Minds and Machines 555 at 575.

[1303] Patricia Conor, «Police resources in Canada, 2017", Statistics Canada (28 March 2018) <https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54912-eng.htm>.

[1304] R v Chehil, 2013 SCC 49 at para 43.

(или известных косвенных значений неизменяемых характеристик) или демонстрирует предвзятость по отношению к определённым группам.

Например, в разделе 9 Хартии считается неконституционным участие в расовом профилировании в качестве основания для задержания. Расовое профилирование может происходить с помощью алгоритмов и негласно узаконено Канадские суды прямо постановили, что расовое профилирование может быть доказано наличием множества факторов, и они не требуют явных доказательств явной предвзятости в сознании полицейского во время задержания. Этот принцип вытекает из признания того, что «установка, лежащая в основе расового профилирования, может быть сознательной или бессознательной, а расовое профилирование может быть продуктом явных, подсознательных или институциональных расовых предубеждений».[1305] Кроме того, расовое профилирование может иметь место, когда «раса используется в сочетании с другими факторами».[1306]

Исторический контекст и сегодняшняя реальность расовых отношений и расового профилирования в Канаде создают, возможно, непреодолимые конституционные препятствия для того, чтобы правоохранительные органы полагались либо на наборы данных, генерируемые полицией, либо на систематически предвзятые наборы данных любого рода для генерации алгоритмически полученных прогнозов, которые используются для оправдания лишения свободы. Верховный суд Канады единогласно принял к сведению судебное уведомление[1307] о производительности значительного объёма исследований, в которых имеет место несоразмерная полицейская деятельность в отношении расовых сообществ и сообществ с низким доходом. о точности значительного объёма исследований, которые установили, что имеет место непропорциональная полицейская деятельность в отношении расовых сообществ и сообществ с низким доходом.[1308] Кроме того, суды также обратили внимание на то, что «полиция по-разному обращается с расовыми меньшинствами и что такое различное отношение не остается для них незамеченным».[1309]Большинство считает, что «в дальнейшем эти отчёты будут явно составлять часть социального контекста при определении того, имело ли место произвольное задержание в нарушение Хартии». [1310]Такие результаты подтверждают фундаментальную необходимость ограничения использования наборов данных, созданных полицией, для прогнозирования совершил ли предполагаемый невиновный человек или может ли он совершить уголовное преступление, а также для оправдания задержаний. Эта потребность ещё более

[1305] R v Neyazi, 2014 ONSC 6838 at para 195.
[1306] Ibid.
[1307] R v Le, 2019 SCC 3, at para 260.
[1308] Ibid at para 97.
[1309] Ibid at para 90.
[1310] Ibid at para 96.

возрастает в контексте системного расизма. Полицейские службы, которые стремятся использовать алгоритмические полицейские технологии, зависящие от базовых полицейских данных, таким образом, столкнутся с проблемами при демонстрации надежности и отсутствия предвзятости в таких системах, а также демонстрации того, что общие подозрения не играют роли в последующих решениях о задержании или аресте кого-либо.[1311] Общеизвестно ненадежная информация не может разумно служить оправданием вмешательства в свободу посредством задержания или ареста.[1312] Подвергание усиленному полицейскому контролю и дополнительным остановкам и задержаниям в результате применения алгоритмических полицейских технологий может усугубить ранее существовавший негативный опыт расовых людей.[1313]Нарушения права на свободу от произвольного задержания часто являются серьёзным и унизительным опытом, который наносит удар по самой сути достоинства личности.

Эти нарушения могут разворачиваться в считанные секунды или минуты, и они могут сказаться на физическом и психическом здоровье человека, повлиять на его способность искать работу и получить образование, способствовать продолжающемуся социально-политическому исключению расовых меньшинств, вызвать потерю доверия к справедливости канадской системы уголовного правосудия и увековечение противоправной и непропорциональной криминализации лиц, которые часто не совершали никаких противоправных действий.[1314]

5.5.3. Заключительные комментарии: алгоритмическая деятельность полиции и право на свободу и свободу от произвольного задержания

В целях соблюдения прав человека и конституционных стандартов правоохранительные органы, которые полагаются на алгоритмические полицейские технологии, не могут использовать их для оправдания вмешательства в свободу (например, арестов или задержаний). По определению, алгоритм прогнозирования основан на обобщённых статистических выводах. Канадский закон требует, чтобы у офицера были разумные подозрения, что конкретное лицо замешано в преступной

[1311] Например, Лум и Айзек продемонстрировали, что алгоритм PredPol приведет к предвзятой и непропорциональной полиции расовых лиц за преступления, связанные с наркотиками, несмотря на аналогичные показатели потребления наркотиков между расовыми и белыми лицами, из-за предвзятости в записанных полицией данных. Кристиан Лум и Уильям Айзек: "Предсказывать и служить?" (2016) 13:5 Значение 14. (2016) 13:5 Significance 14.

[1312] R v Nuttall, 2018 BCCA 479, at para 244; R v Bernshaw, [1995] 1 SCR 254.

[1313] R v Le, 2019 SCC 34, at para 95

[1314] Ibid.

деятельности, чтобы оправдать своё задержание или арест. Подозрение должно быть связано с конкретными характеристиками и поведением данного человека. Кроме того, подозрения не обоснованы, если они основаны на неизменных характеристиках, таких как раса. Правоохранительные органы, применяющие алгоритмические полицейские технологии, должны гарантировать, что такие методы на практике не расширяют рамки того, что считается «разумным» подозрением, особенно в случае расовых или других маргинализированных сообществ, которые уже подвергаются необоснованным подозрениям в форме неосознанной предвзятости и расового профилирования в системе уголовного правосудия.

Право на надлежащую правовую процеду

Право на надлежащую правовую процедуру является основополагающим принципом в системе уголовного правосудия и закреплено в международном праве прав человека и в Хартии. Статья 14 МПГПП защищает определенные права на надлежащую правовую процедуру, такие как право считаться невиновным до тех пор, пока его вина не будет доказана в ходе беспристрастного разбирательства дела в суде.[1315] Раздел 7 Хартии гарантирует, что все люди имеют право на жизнь, свободу и личную неприкосновенность, которые не могут быть ограничены «иначе, как в соответствии с принципами фундаментальной справедливости».[1316] Принципы фундаментального правосудия – это основополагающие, организующие принципы и ценности, которые составляют основу того, как должна работать система правосудия.[1317] Например, один конкретный принцип фундаментального правосудия в соответствии с разделом 7 - это право на полный ответ и защиту по уголовному обвинению. Защита прав на надлежащую правовую процедуру в разделе 7 подкрепляется другими правами в Хартии, которые касаются хабеас корпус (определение законности ареста или задержания), права на разумный залог, право не подвергаться произвольному задержанию и аресту и право на справедливое судебное разбирательство.[1318] Использование алгоритмической полицейской технологии правоохранительными органами поднимает ряд конституционных вопросов и проблем с правами человека в связи с правом на надлежащую правовую процедуру, которые будут проанализированы в

[1315] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 14.
[1316] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 7.
[1317] Canada (Attorney General) v. Bedford, 2013 SCC 72, at para. 94-96.
[1318] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c11, ss 9, 10(c), and 11(e).

следующих подразделах этого отчёта. В разделе 5.6.1 обсуждается концепция алгоритмической прозрачности и связь между доступом к информации и способностью человека осуществлять свои права на надлежащую правовую процедуру. Право на надлежащую правовую процедуру задействовано в тех случаях, когда люди, на которых действует алгоритм технологии, не могут получить необходимую информацию для оценки надежности технологии, поэтому они не могут определить, были ли нарушены их права в результате её использования. В разделе 5.6.1 также представлены опасения относительно влияния поставщиков из частного сектора на доступ к информации и соблюдение процессуальных прав. В разделе 5.6.2 исследуется, как технологии алгоритмического контроля могут повлиять на право давать полный ответ и защиту, включая роль раскрытия информации (т.е. раскрытие правоохранительными органами того, что такая технология использовалась в конкретном случае).

5.6.1. Информационные барьеры для надлежащей правовой процедуры: алгоритмическая прозрачность и влияние частного сектора

Использование правоохранительными органами алгоритмической полицейской технологии вызывает озабоченность в связи с соблюдением процессуальных норм в тех случаях, когда существуют препятствия для раскрытия информации о технологии. Информационная асимметрия между правоохранительными органами, использующими алгоритмические полицейские технологии, и отдельными лицами, и сообществами, на которые они оказывают непропорциональное и негативное влияние, поднимает проблему алгоритмической прозрачности. Концепция алгоритмической прозрачности является частью более широкой системы принципов, которые обычно называют алгоритмической справедливостью, подотчетностью, прозрачностью и этикой (FATE).[1319] Хотя стало широко признанным, что алгоритмическая прозрачность сама по себе не обязательно означает алгоритмическую подотчётность без дальнейших действий,[1320] прозрачность

[1319] Эти широкие принципы были разработаны и усовершенствованы с помощью значительного объема литературы, информационно-пропагандистской деятельности, правительственных и отраслевых инициатив и двух крупных ежегодных конференций. See e.g., «Fairness, Accountability, and Transparency in Machine Learning", <https://www. fatml.org>; European Parliamentary, European Parliamentary Research Service, «A governance framework for algorithmic accountability and transparency", (April 2019) <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf>; Robert H Sloan & Richard Warner, «When Is an Algorithm Transparent? Predictive Analytics, Privacy, and Public Policy", (May/June 2018) 16:3 IEEE Security & Privacy 18 <https://ieeexplore.ieee.org/document/8395116>.

[1320] See e.g., Maayan Perel & Niva Elkin-Koren, «Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement" (2017) 69:1 Florida Law Review 181; and Janelle Berscheld & Francois Roewer-Despres, «Beyond Transparency: A Proposed Framework for Accountability in Decision¬Making AI Systems" (2019) 5:2 AI Matters 13.

часто является предварительным условием достижения подотчётности, а отсутствие прозрачности требует особого внимания. Обеспечение прозрачности с помощью технологий алгоритмического контроля может быть сложной задачей, если не невозможной, из-за природы самой технологии. Методы машинного обучения «значительно различаются по степени прозрачности, которую они могут обеспечить», поскольку некоторые «формы машинного обучения предоставляют гораздо меньше информации о том, как модель вычисляет результат».[1321]

В некоторых случаях даже разработчик алгоритмической технологии может быть не в состоянии объяснить, как алгоритм пришёл к сгенерированному им решению. Например, обсуждая систему алгоритмического прогнозирования GeoDASH Департамента полиции Ванкувера, констебль Райан Прокс поделился, что «офицеры VPD запускают свой алгоритм в режиме машинного обучения с интервалами в 3 недели; каждые 3 недели он переписывает его алгоритмический код. Вот почему мы проводим независимые аудиты. Потому что я не могу сказать вам, какие факторы он взвешивает в соответствии с определениями для ящиков. Я могу сказать вам, делает ли он это правильно, основываясь на том, где происходят инциденты, но я не могу сказать вам «почему» и какое значение это имеет для каких факторов».[1322]

Растущее партнерство между частным бизнесом и правоохранительными органами создает особые проблемы в отношении прозрачности и соблюдения процессуальных прав. Частные компании часто сопротивляются или отказываются предоставить полное и значимое раскрытие информации о своих инструментах алгоритмического контроля, включая информацию о лежащих в основе алгоритмических моделях, переменных, используемых наборах данных и тестировании, которое говорит об уровне надёжности и точности инструмента. В то же время поставщики полицейских технологий вносят свой

[1321] Alexander Babuta, Marion Oswald and Christine Rinik, «Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges" (September 2018) RUSI Whitehall Report 3-18, <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_ algorithms.pdf.pdf>. See also, UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40; «Can we open the black box of AI?", https:// www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731. Проблема "черного ящика" включает в себя, например, невозможность рассказать или объяснить, на какие факторы полагался алгоритм для принятия решения, или незнание, насколько или насколько мало вес алгоритм присваивал различным факторам при его определении. Появляется растущее поле, которое пытается "решить" проблему черного ящика путем разработки "объяснимого ИИ" (XAI); однако еще предстоит выяснить, в какой степени эта линия расследования отвечает такому обещанию. See e.g., Amina Adadi & Mohammed Berrada, «Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)", (2018) IEEE Access <https://ieeexplore.ieee.org/stamp/ stamp.jsp?arnumber=8466590>; AJ Abdallat, «Explainable AI: Why We Need To Open The Black Box", Forbes (22 February 2019) <https://www. forbes.com/sites/forbestechcouncil/2019/02/22/explainable-ai-why-we-need-to-open-the-black- box/#75d712771717>; however, see, e.g., Cassie Kozyrkov,."Explainable AI won't deliver. Here's why.", Hackernoon (16 September 2018) <https://hackernoon.com/explainable-ai-wont-deliver- here-s-why-6738f54216be>.

[1322] Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

вклад в снижение прозрачности начального процесса закупок, негласно лоббируя правительственные агентства с целью приобретения, принятия или продвижения их продукции. [1323] Законы о коммерческой тайне и другие законы об интеллектуальной собственности также создают существенные препятствия для принципов FATE при принятии алгоритмических решений.[1324]Например, когда VPD впервые реализовал GeoDASH APS, он был представлен наблюдательному совету VPD для защиты вовлечённых частных коммерческих интересов.[1325]

Обеспокоенность несвободным программным обеспечением повлияла на решение SPPAL разработать собственную технологию алгоритмического контроля: Не говоря за всех партнёров, изначально мы начали, потому что мы были обеспокоены характером черного ящика проприетарного программного обеспечения. С консультацией университета и нашим чувством, что мы могли бы разработать что-то более прозрачное, и, возможно, даже более современным способом, мы отказались от этого. Вот где мы сейчас находимся, особенно для этого проекта. Это не значит, что в будущем некоторые вещи нельзя будет рассматривать. Но на данный момент это было сознательное усилие, чтобы сделать это собственными силами, чтобы мы могли быть максимально прозрачными, чтобы мы могли анализировать и защищать это.[1326]

Судебные разбирательства в Соединенных Штатах, касающиеся технологии оценки рисков COMPAS, служат поучительным примером того, как принципы надлежащей правовой процедуры не всегда соблюдались или отдавались приоритетом с самых ранних стадий потенциальной закупки или использования. В деле Государство против Лумиса, штат Висконсин, не

[1323] Например, лоббист, нанятый Shotspotter, продавцом алгоритмической системы обнаружения огнестрельного оружия, был зарегистрирован в городе Торонто с 2013 года и имел множественные связи с двумя городскими советниками и мэром Джоном Тори и их сотрудниками в период с 2013 по 2016 год. Впоследствии генеральный директор Shotspotter Ральф Кларк и три других высокопоставленных руководителя зарегистрировались в качестве лоббистов всего через несколько дней после ходатайства мэра Тори в Совет полицейских служб Торонто о финансировании для лицензирования программного обеспечения Shotspotter в Торонто. City of Toronto, <http://app.toronto.ca/ lobbyistsearch/searchInput.do> (available by searching with keyword «ShotSpotter", accessed 1 October 2019); «Could a Controversial Gun Surveillance System Help Tackle Toronto Crime?", The Globe and Mail, <https://www.theglobeandmail.com/news/toronto/technology-offers- police-more-than-a-shot-in-the-dark/article307730 05/>; and Jessica Patton, What is 'ShotSpotter'? Controversial gunshot detector technology approved by Toronto police", Global News (20 July 2018). In Massachusetts, a facial recognition company called Suspect Technologies offered to provide its product to the local police department for free, in exchange for the department's support on a government grant application. Joseph Cox, «'They Would Go Absolutely Nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work With Cops", VICE Motherboard (6 May 2019) <https://www.vice.com/en_ca/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies>.

[1324] Тем не менее, см. объяснение Эндрю Селбста о том, что коммерческие секреты не всегда могут препятствовать алгоритмической прозрачности в контексте алгоритмических оценок воздействия; но там, где они это делают, "нет никаких причин, в качестве политического вопроса, почему коммерческая тайна должна иметь преференциальный статус по сравнению с чем-то таким важным, как справедливость в уголовном правосудии". Andrew D. Selbst, «Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 190. See also

[1325] Ibid.

[1326] Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

предоставил раскрытие информации о том, как инструмент оценки рисков COMPAS использовался в деле ответчика[1327], включая информацию о том, «как [были] определены оценки риска или как [были] взвешены факторы».[1328] Раскрытие информации не было предоставлено, поскольку поставщик COMPAS, Northpointe, Inc. (ныне EquivantЭквивалент) заявил о своих правах собственности.[1329] Верховный суд штата Висконсин постановил, что использование алгоритмической оценки риска при вынесении приговора не нарушает права обвиняемого на надлежащую правовую процедуру, несмотря на отсутствие раскрытия информации[1330]и несмотря на признание того, что исследования, проверяющие прогнозы COMPAS, «вызывают озабоченность относительно того, как факторы риска оценки COMPASS коррелируют с расой».[1331] Одно исследование показало, что «чернокожие обвиняемые гораздо чаще, чем белые обвиняемые, были ошибочно признаны подверженными более высокому риску рецидивизма ... [в то время как] белые обвиняемые с большей вероятностью, чем черные обвиняемые были неправильно отмечены как низкий уровень риска».[1332] Даже если Канада примет законы, требующие раскрытия информации от поставщиков, торговые соглашения могут заблокировать возможность применения условий на стадии закупок или импорта.[1333] Исключения применяются только в контексте конкретных расследований и дел, и даже в этом случае они остаются «под защитой от несанкционированного раскрытия информации».[1334] Эта ситуация означает, что, если технология алгоритмического контроля базируется в Соединенных Штатах или Мексике, правительству Канады может быть запрещено требовать полной алгоритмической прозрачности на стадии закупок. Скорее, алгоритмы, лежащие в основе технологии, не могли быть исследованы до тех пор, пока не был нанесён ущерб и не началось фактическое разбирательство – возможно, даже тогда и, почти наверняка, не без дальнейших препятствий в получении необходимой информации.

[1327] The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is a risk-assessment tool designed to provide «decisional support" for the Department of Corrections when making placement decisions, managing offenders, and planning treatment.

[1328] State v Loomis, 881 NW 2d 749 (Wis 2016) at para 51.

[1329] State v Loomis, 881 NW 2d 759 (Wis 2016) at para 51.

[1330] State v Loomis, 881 NW 2d 769 (Wis 2016).

[1331] State v Loomis, 881 NW 2d 779 (Wis 2016).

[1332] State v Loomis, 881 NW 2d 750 (Wis 2016) at para 63.

[1333] Статья 19.16.1 Соглашения между Канадой и Соединенными Штатами Америки и Мексикой (CUSMA) запрещает странам-членам требовать "доступа" к исходному программному коду или алгоритмам программного обеспечения, базирующимся в других странах, в качестве условия "импорта, распространения, продажи или использования" этого программного обеспечения в стране. Canada-United States-Mexico Agreement, 30 November 2018 (ratified 13 March 2020), Art 19.16, para 1, <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>.

[1334] Статья 19.16.2 предусматривает, что регулирующий орган или судебный орган может потребовать от владельца "сохранения и предоставления исходного кода программного обеспечения или алгоритма, выраженного в этом исходном коде, регулирующему органу для проведения конкретного расследования, инспекции, экспертизы, принятия принудительных мер или судебного разбирательства". Canada-United States-Mexico Agreement, 30 November 2018 (ratified 13 March 2020), Art 19.16, para 2.

Эти соображения должны быть приняты во внимание при регулировании и потенциальной реализации алгоритмического контроля, например, путём запрещения закупки коммерческих готовых алгоритмических технологий контроля у поставщиков, базирующихся в США или Мексике, или у любых поставщиков, которые не хотят или не могут обеспечить уровень прозрачности, необходимый для защиты конституционных прав и прав человека при их использовании в Канаде.

При рассмотрении вопроса о приобретении или использовании технологии алгоритмической полицейской деятельности канадские правительства, законодатели и органы уголовного правосудия должны проявлять бдительность и уделять приоритетное внимание правам на надлежащую правовую процедуру лиц, подпадающих под действие системы уголовного правосудия. Как признает федеральное министерство юстиции, «можно предположить, что, если процессуальные меры защиты применяются вне уголовного контекста, они применяются с большей силой в уголовном контексте».[1335] Правовые стандарты, представляющие общественный интерес, должны применяться к коммерческим поставщикам, которые заключают контракты с правительством или правоохранительными органами, когда на карту поставлена уголовная опасность. Неоправданно отдавать приоритет имущественным интересам или прибыли за счёт человеческих и конституционных прав человека, таких как право не быть лишённым свободы, иначе как в соответствии с принципами фундаментальной справедливости.[1336]

В фокусе внимания № 7

Алгоритмы с открытым исходным кодом и обзор исходного кода

Что касается государственной подотчётности и государственного финансирования, то государственные и правоохранительные органы, разрабатывающие полицейские технологии – как собственные, так и в партнерстве с частными инвесторами – должны сделать исходный код и связанные с ним детали общедоступными в машиночитаемом виде и читаемой форме. Это способствовало бы созданию значимых прав на надлежащую правовую процедуру и средство правовой защиты. Обнародование исходного кода алгоритмической полицейской технологии также способствовало бы информированному участию общественности в содержательном

1335 ……

1336 ……..

демократическом диалоге относительно того, следует ли применять ту или иную технологию в правоохранительных целях. Одним из возможных механизмов, с помощью которого можно было бы реализовать политику открытого исходного кода, является применение лицензированного программного обеспечения с открытым исходным кодом, таким как GNU General Public License (GPL) к программному обеспечению, стоящему за технологиями алгоритмической политики.[1337]

Открытое лицензирование программного обеспечения было бы уместно в тех случаях, когда технологии финансируются государством, следовательно, должны быть доступны представителям общественности для целей обзора или исследования. Возможно, существуют некоторые виды алгоритмических технологий контроля, для которых выпускать исходный код для общественности или делать его открытым исходным кодом было бы противоречащим общественным интересам.

В тех случаях, когда это обстоятельство может быть доказано, исходный код и связанные с ним детали должны быть по-прежнему доступны соответствующим государственным органам и независимым экспертам на конфиденциальной основе. Эта доступность необходима в целях проведения алгоритмических оценок воздействия, предварительной проверки закупок и текстов на наличие уязвимостей в системе безопасности. Аналогичным образом, в тех случаях, когда любая технология была разработана или принята и введена в действие, исходный код должен быть конфиденциально доступен для аудита. В ходе расследований и судебных разбирательств широкое обоснование такой конфиденциальности должно быть обнародовано и запутано надзорными группами, такими как уполномоченным по вопросам информации или конфиденциальности.

Учреждения и частные лица, которым предоставляется доступ к исходному коду для целей проверки и аудита, могут быть связаны обязательствами конфиденциальности в отношении содержания самого исходного кода, но они не должны быть связаны обязательствами конфиденциальности в отношении своих выводов, основанных на исходном коде.

Государственные и правоохранительные органы, приобретающие готовые технологии алгоритмического контроля, но не участвующие в разработке какой-либо из приобретенных технологий, должны в качестве условия закупки включать в контракты отказ поставщика от коммерческой тайны и связанных с ней прав собственности. Эти права должны быть отменены для всех версий

[1337] «GNU General Public License", GNU Operating System (18 November 2016) <https://www.gnu.org/licenses/gpl-3.0.en.html>; and «About The Licenses", Creative Commons <https://creativecommons.org/licenses/>.

проприетарных программных компонентов в той степени, которая позволяет государственным органам и независимым экспертам осуществлять доступ и тестирование алгоритмических технологий.

Такой отказ включает в себя отказ от права собственности для соответствующего правительства или правоохранительного органа, что позволит им проводить независимые аудиты исследований, проверок, экспертиз, правоохранительных действий или судебного производства. Этот процесс также будет подлежать гарантиям против несанкционированного раскрытия информации, если не разглашение информации общественности будет признано соображениями общественного интереса.

Претворение этой рекомендации в жизнь могло бы, в качестве примера, задействовать канцелярию конфиденциального комиссара, канадский центр кибербезопасности или федеральные исследовательские агентства как государственные органы, ответственные за пересмотр управления алгоритмическими технологиями в рамках процесса закупок.

5.6.2. Неразглашение и право на полный ответ и защиту

Право на полный ответ и защиту по уголовному обвинению – компонент защиты надлежащей правовой процедуры – является одним из принципов основополагающего правосудия в соответствии с разделом 7 Хартии.[1338] Этот принцип налагает на обвинение Короны обязанность раскрывать всю соответствующую информацию в его распоряжении или под контролем обвиняемых по уголовному делу.[1339] Без полного раскрытия такой информации или если полное раскрытие невозможно, использование алгоритмической полицейской технологии, которая приводит к вмешательству в свободу человека, рискует получить неправомерные приговоры в системе уголовного правосудия и нарушит право на надлежащую правовую процедуру. Нарушение прав на надлежащую правовую процедуру при неразглашении информации о технологии алгоритмического контроля определяется контекстом. Объём прав на надлежащую правовую процедуру зависит от характера опасности для лица (т.е. от того, какие интересы, защищенные Уставом, были затронуты или

[1338] Право дать полный ответ и защиту является дополнением к праву на справедливое судебное разбирательство, которое само по себе также гарантируется разделом 11 (d) Хартии.

[1339] Корона обязана раскрывать всю информацию, имеющуюся в распоряжении Короны, осуществляющей судебное преследование (за исключением случаев, когда она явно не имеет значения, привилегирована или ее раскрытие иным образом регулируется законом), а также результаты расследования, находящегося во владении полиции: R vStinchcombe, [1991] 3 SCR 326; R vMcNeil, [2009] 1 SCR 66. Relevant information includes information that speaks to the merits of the allegations; exculpatory information or information that may assist the defence in its own investigation or preparation for trial; and information relevant to Charter issues or remedies arising in the case: R vStinchcombe, [1991] 3 SCR 326; R v Jackson, 2015 ONCA 832.

поставлены на карту); какие потенциальные возражения или требования Устава могут быть задействованы; и является ли использование правоохранительными органами технологии алгоритмического наблюдения спорным вопросом. Определение права человека на надлежащую правовую процедуру и на полный ответ и защиту в отношении использования конкретных технологий повлечёт за собой очень контекстные запросы. Чтобы проиллюстрировать противоречия, которые влияют на то, соответствует ли использование алгоритмической полицейской технологии праву на надлежащую правовую процедуру, в этом подразделе основное внимание уделяется одному из основных источников надлежащей правовой защиты: праву дать полный ответ и защите в тех случаях, когда государство стремится ограничить права человека. Когда дело доходит до технологии алгоритмического контроля, любая оценка права на раскрытие обязательно подразумевает принцип алгоритмической прозрачности. В контексте уголовного дела алгоритмическая прозрачность требует определения того, какая информация должна быть раскрыта, чтобы защитить право давать полный ответ и защиту лица, на которого повлияла технология алгоритмической полицейской деятельности. Корона должна быть обязана раскрывать следующие типы информации, чтобы ответчик мог оценить надёжность технологии, а также любые применимые проблемы Устава и средства защиты, связанные с использованием инструмента:

- Как работает инструмент и лежащие в его основе алгоритмические модели (если разработчики не могут сказать, как работает инструмент или его алгоритмы, они должны указать это явно);
- На каких наборах данных обучались алгоритмы;
- Право дать полный ответ и защиту является дополнением к праву на справедливое судебное разбирательство, которое само по себе также гарантируется разделом 11 (d) Хартии.
- Как алгоритм взвешивает различные факторы (если разработчики не могут определить, как алгоритм взвешивает различные факторы, они должны указать это явно);
- Какие исходные данные использовались;
- Информация об отношениях и любых контрактах, меморандумах о взаимопонимании или соглашениях между правоохранительными органами и сторонними субъектами частного сектора, которые участвовали в сборе данных или анализе данных, на которые правоохранительные органы полагались до предъявления уголовного обвинения;
- Информация о взаимоотношениях и любых контрактах, меморандумах о взаимопонимании или соглашениях между правоохранительными органами и сторонними поставщиками инструментов алгоритмического контроля, которые правоохранительные

органы приобрели в готовом виде или разработали в сотрудничестве с частным поставщиком;

- Информация о методах и практиках тестирования и обслуживания, используемых разработчиком, включая всю доступную информацию, касающуюся надежности или точности прогнозов, или решений, сгенерированных инструментом при тестировании и/или предыдущих сценариях использования (например, степень точности инструментов прогнозирования рецидивов), точность средств распознавания лиц).

Как указано в разделе 5.6.1 («Информационные барьеры для надлежащей правовой процедуры: алгоритмическая прозрачность и влияние частного сектора»), препятствия для раскрытия информации могут возникать в зависимости от характера технологии или наличия прав собственности со стороны частных поставщиков. Если полное раскрытие всей соответствующей информации невозможно (например, из-за заявления стороннего поставщика о правах собственности или неспособности разработчика определить на техническом уровне и простым языком, как работает алгоритм), использование правоохранительными органами этой технологии таким образом, который затрагивает свободу человека или другие интересы, охраняемые Уставом, несовместимо с правом на полный ответ и защиту. Ключевая особенность прав на надлежащую правовую процедуру связана с всеобъемлющим принципом Хартии, согласно которому, если государство вмешивается в свободу человека, оно может сделать это только разумным образом.[1340] Если алгоритмический инструмент используется для формирования оснований для лишения свободы и является ненадежным или предвзятым, он не может разумно служить оправданием лишения свободы или других затронутых прав.

Коронеры несут бремя доказательства того, что ограничения свободы разумно оправданы. В результате для того, чтобы коронеры осмысленно несли свое бремя, а для обвиняемых, адвокатов, судов и общественности, чтобы иметь возможность тщательно проверять надежность и использование алгоритмической полицейской технологии правоохранительными органами, доступ к значимому раскрытию информации является критически важным. Когда коронеры пытаются представить доказательства, полученные с помощью

[1340] Право на свободу, защищаемое статьей 7, подкрепляется целым рядом мер защиты, которые обеспечивают разумные основания для всех случаев лишения свободы. Эти меры защиты проявляются на различных этапах уголовного процесса с момента первого обращения лица в полицию до вынесения и завершения приговора, если оно признано виновным. Например, после этапа охраны порядка на переднем крае статья 11 e) гарантирует, что все лица, обвиняемые в совершении преступления, имеют право не быть лишенными разумного залога без уважительной причины, а презумпция невиновности защищается статьей 11.d) Хартии означает, что лицо не может быть подвергнуто тюремному заключению за преступление, если только Корона не установит вину вне всяких разумных сомнений в ходе справедливого судебного разбирательства. Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, ss 9, 11(d), and 11(e).

технологии алгоритмического контроля, необходимо предоставить доступ к раскрытию информации.

В таких ситуациях нераскрытие информации, вероятно, подорвёт способность коронера выполнить своё обязательство демонстрации того, что любые ограничения личной свободы были или будут разумно оправданы. Невыполнение этого обязательства нарушит право обвиняемого на дачу полного ответа и защиту, лишив этого человека и его адвоката соответствующей информации относительно оправданности лишения свободы.

Любое нарушение права на полный ответ и защиту при использовании алгоритмической полицейской технологии имеет серьезные последствия для тех, кто стал мишенью этой технологии, и для общественного доверия к отправлению правосудия. Технология алгоритмического контроля – это постоянно развивающаяся область, и надежность этих технологий повсеместно не является фактом или научным консенсусом.[1341] Фактически, Департамент полиции Чикаго завершил свой список стратегических объектов (SSL) в январе 2020 года, после того как Управление Генерального инспектора города выпустило рекомендацию, в которой ставится под сомнение его надежность,[1342] и Департамент полиции Лос-Анджелеса завершил программу L.A. Strategic Extraction and Restoration – Стратегической добычи и восстановления (LASER) в марте 2019 года, [1343] после того, как его генеральный инспектор завершил аудит, который выявил «отсутствие чётких и надёжных данных, которые можно было бы использовать для измерения как затрат, так и результатов» программы.[1344]Вопросы о надёжности таких технологий являются существенными, особенно в свете проблем, которые были подняты учёными, непропорционально сильно затронутыми сообществами и исследователями в области прав человека. Обеспокоенность относительно уместности

[1341] Например, обзор существующей литературы за 2019 год выявил только четыре эмпирических исследования методов прогнозной полицейской деятельности и пришел к выводу, что «нынешняя направленность инициатив прогнозирующей полицейской деятельности основана на убедительных аргументах и анекдотических данных, а не на систематических эмпирических исследованиях». Кроме того, авторы определили, что эмпирическая литература была сосредоточена на оценке преимуществ алгоритмической полицейской работы и не учитывала оценку неблагоприятных эффектов. Albert Meijer & Martijn Wessels, «Predictive Policing: Review of Benefits and Drawbacks" (2019) 42:12 International Journal of Public Administration, 1031-1039 at 1037 <https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664>.

[1342] Jeremy Gorner & Annie Sweeney, «For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended", Chicago Tribune (24 January 2020), <https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police- strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html>; and «Advisory Concerning the Chicago Police Department's Predictive Risk Models", City of Chicago Office of Inspector General (23 January 2020) <https://igchicago.org/wp-content/uploads/2020/01/ OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf>.

[1343] Mark Puente, «LAPD to scrap some crime data programs after criticism", Los Angeles Times (5 April 2019) <https://www.latimes.com/local/ lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html>.

[1344] Mark P Smith, «Review of Selected Los Angeles Police Department Data-Driven Policing Strategies", Office of the Inspector General, Los Angeles Police Commission (12 March 2019), at 23. <https://a27e0481-a3d0-44b8-8142-1376cfbb6e32.filesusr.com/ugd/ b2dd23_21f6fe20f1b84c179abf440d4c049219.pdf>. The report also raised concerns about the LAPD's use of PredPol, including discrepancies in data collection which «made it difficult to draw conclusions about the effectiveness of the system in reducing vehicle or other crime". Ibid, at 29.

используемых наборов данных включает вопросы об источнике и возрасте данных, размере выборки данных, демографии тех, которые отражены в данных, и точности самих наборов данных.[1345]Проблемы также связаны с потенциальным присутствием системных предубеждений в наборах данных, которые впоследствии используются для обучения или в качестве входных данных для рассматриваемой технологии алгоритмического контроля.[1346]

Сравнение алгоритмических полицейских технологий с использованием экспертных заключений в системе уголовного правосудия может обеспечить основу и наводящие вопросы, на которые суды будут ссылаться при оценке надёжности таких технологий. Обладая экспертными показаниями, суды выполняют важную функцию привратника, гарантируя, что допущенные доказательства являются достаточно надёжными, не узурпируют судью или присяжных и не рискуют предвзято относиться к эксперту. Учитывая риски неправомерного осуждения, связанные с представлением экспертных заключений, в дополнение к другим вопросам, которые могут повлиять на процессуальную справедливость в уголовном судопроизводстве, появился большой свод законов, регулирующих использование таких доказательств.[1347] Соответствующий закон признает, что экспертные показания должны быть квалифицированными (т.е. считается, что эксперт должен обладать надлежащими знаниями, чтобы высказать своё мнение суду по рассматриваемому вопросу) и оценены соответствующим образом для определения их приемлемости в уголовном судопроизводстве. Во многих отношениях использование алгоритмических полицейских технологий в уголовном судопроизводстве сродни использованию неквалифицированных экспертных заключений. Доступ к содержательному и полному раскрытию информации о технологии имеет решающее значение для суда, чтобы иметь возможность выполнять свою роль привратника над использованием экспертных заключений.

Подобно экспертам, которые могут узурпировать роль судьи или придать своим показаниям излишний вес в глазах суда, инструментам алгоритмической полицейской деятельности может быть придан чрезмерный вес, учитывая значительные риски предвзятости автоматизации,[1348] которые связаны с

[1345] Logan Koepke & David Robinson, «Danger Ahead: Risk Assessment and the Future of Bail Reform" (2019) 93 Washington Law Review 1725; Innocence at Stake: The Need for Continued Vigilance to Prevent Wrongful Convictions in Canada (2018) <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf>, at p 169-172 (recognizing the phenomenon of false guilty pleas in criminal courts, which will taint criminal record data).

[1346] Danielle Groen, «How We Made AI As Racist and Sexist As Humans", The Walrus (4 October 2019) <https://thewalrus.ca/how-we-made-ai-as-racist-and-sexist-as-humans/>.

[1347] Комиссии по расследованию неоднократно подчеркивали важность надлежащей правовой защиты после вынесения громких обвинительных приговоров в отношении противоправных деяний. Именно там, где нарушаются эти меры защиты, обвиняемые подвергаются большему риску неправомерного осуждения: «Thomas Sophonow Inquiry Report",
<https://digitalcollection.gov.mb.ca/awweb/pdfopener?smd=1&did=12713&md=1>; Truscott (Re), 2007 ONCA 575.

[1348] Hannah Couchman, «Policing by Machine: Predictive policing and the threat to our rights," (January 2019) Liberty,

алгоритмической технологией.[1349] Чтобы смягчить такую предвзятость, должно быть полное раскрытие того, как работают различные инструменты, и выявление скрытых проблем надёжности в рамках конкретной алгоритмической технологии. Такое раскрытие информации также необходимо для того, чтобы участники системы правосудия не испытывали ложного чувства безопасности относительно способности или целесообразности полагаться на такие технологии при принятии решений, которые влияют на гражданские свободы и конституционные права людей.

Более того, люди, которые фактически создают технологию алгоритмического контроля, могут быть потенциально неквалифицированными экспертами. Чан и Беннет Мозес описали, как рост больших данных побудил некоторых энтузиастов принять корреляцию, а не причинную связь, предвещая «возникающий «юрисдикционный конфликт» между социологами и аналитиками больших данных»,[1350] в том числе в криминологии. Келли Ханна-Моффат изучила движение в инструментах оценки криминального риска от «риска с учётом психологии» к «риску с учётом больших данных». [1351]

Технологи (например, заинтересованные граждане, компьютерные учёные, инженеры-программисты и хакеры - обычно не имеющие образования в области социальных наук), которые делают данные общедоступными и доступными для ряда заинтересованных сторон».[1352]

Участие технологических компаний и разработчиков, не относящихся к криминалистике, уголовному праву и системе уголовного правосудия, вызывает давние опасения по поводу воздействия техноцентрических или техно-солюшенских взглядов на уголовное правосудие.[1353]Всё чаще системы и

---

at 34<https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf.

[1349] Смещение автоматизации обсуждается в разделе 5.5.1 ("Алгоритмическая политика и обобщенное подозрение") и определяется как склонность человека "полагаться на суждения автоматизированных решений как превосходящие свои собственные, даже если у них есть основания полагать, что технология является ошибочной". Lindsey Barrett, «Reasonably Suspicious Algorithms: Predictive Policing at the United States Border", (2017) 41 NYU Review of Law & Social Change 327 <https://socialchangenyu.com/wp-content/uploads/2017/09/barrett_digital_9-6-17.pdf> at 342-43. See also Danielle Keats Citron, «Technological Due Process" (2008) 85:6 Washington Law Review 1249 at 1271-1272, <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview>.

[1350] Janet Chan & Lydia Bennett Moses, «Is Big Data challenging criminology?" (2016) 20:1 Theoretical Criminology 21 at 23.

[1351] Первый из них разработан на основе целенаправленной разработки, установленных методологий социальных наук и дисциплинарных знаний и стандартов, в то время как второй связан с "методологическими неопределенностями" и "данными, которые собираются и разбираются для целого ряда целей и разрабатываются без увязки с конкретной дисциплиной". Kelly Hannah-Moffat, «Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates" (2018) 23:4 Theoretical Criminology 453 at 458.

[1352] Ibid, at 456.

[1353] Смотрите, например, "Эта тенденция [к автоматизированному принятию решений] является частью" алгоритмической управляемости "(Rouvroy and Berns, 2013) и возросшего влияния математики на все сферы нашей жизни (O 'Neil, 2016). Это часть "решения", в соответствии с которым технологические компании предлагают технические решения всех социальных проблем, включая преступность. (Morozov, 2013)." Ales

методы охраны правопорядка и принятие решений правоохранительными органами продвигаются через технологический сектор, отрасль науки о данных и частные предприятия, которые не обязательно обладают опытом в определённой области или руководствуются теми же ценностями, которые лежат в основе целей уголовного правосудия. Такие области и их участники также могут не подпадать под действие необходимых профессиональных правил, этических стандартов или аналитических требований, связанных с криминологическими исследованиями или экспертизой государственной политикой в области полицейской деятельности и уголовного правосудия, или не обучаться им.[1354] Отсутствие опыта, вероятно, будет более серьезной проблемой, когда правоохранительные органы приобретают готовые продукты или услуги у частных компаний, в отличие, например, от того, как VPD разработал свою систему алгоритмического прогнозирования GeoDASH в сотрудничестве с университетскими академиками и частными продавцами.[1355] Точно так же проекты прогнозирующей полицейской службы SPPAL проводятся в соответствии с протоколами, установленными Советом по этике исследований Университета Саскачевана.[1356]

Включение независимых и авторитетных академических и отраслевых экспертов в разработку технологий алгоритмического контроля – важный первый шаг к увеличению шансов на надёжность технологии. Однако прямое

Zavrsnik, «Algorithmic justice: Algorithms and big data in criminal justice settings" (2019) European Journal of Criminology 1 at 2. See generally Evgeny Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism (New York: PublicAffairs, 2013) and Meredith Broussard, Artificial Unintelligence: How Computers Misunderstand the World (Cambridge, MA: MIT Press, 2018).

[1354] Одним из особенно тревожных результатов участия в технологическом развитии отдельно от этических соображений и исторического и социально-политического контекста, в том числе в области уголовного правосудия, является попытка людей разработать алгоритмические технологии, которые предназначены для прогнозирования конфиденциальной личной информации о человеке только на основе его черт лица, например, являются ли они преступником или какова их сексуальная ориентация - потенциально «возрождая старую веру с плохой историей: вы можете интуитивно понять характер персонажа по внешнему виду. Эта псевдонаука, физиогномика, была топливом для научного расизма 19-го века. и 20 века, и давала моральное прикрытие некоторым из худших импульсов человечества». James Vincent, «The invention of AI 'gaydar' could be the start of something much worse", The Verge (21 September 2017) <https://www.theverge. com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy>; see also Sahil Chinoy, «The Racist History Behind Facial Recognition", New York Times (10 July 2019) <https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html> («The technological frontiers being explored by questionable researchers and unscrupulous start-ups recall the discredited pseudosciences of physiognomy and phrenology, which purport to use facial structure and head shape to assess character and mental capacity.") As an example of one such concerning technological endeavour, see Parabon NanoLabs: «Algorithmic DNA Sketches", <https://parabon-nanolabs.com/>; Emerging Technology from the arXiv, «Neural Network Learns to Identify Criminals by Their Faces", Technology Review (22 November 2016) <https://www.technologyreview.com/sZ602955/ neural-network-learns-to-identify-criminals-by-their-faces/>.

[1355] По словам Прокса, частный поставщик удовлетворял потребности в технологиях, которые были "приемлемыми для промышленности и стандартизированными", но также отметил: "Это стало намного сложнее, когда мы привлекли частный сектор", по сравнению с первоначальным партнерством между VPD и только академиками. Интервью Райана Прокса Синтии Хоо и Йоланды Сонг (7 May 2019).

[1356] IИнтервью представителя Saskatchewan Police Predictive Analytics Lab (SPPAL) Синтии Кхоо (23 июля 2019 года). Представитель также заявил: "Мы любим проверять [алгоритмические модели SPPAL] на других образцах или заставлять других людей смотреть, видеть, как они [модели] работают, использовать другие методы, видеть, одобряют ли они или нет. Вы хотите убедиться, что то, что вы находите, является надежным, но также открыт для изучения".

участие таких экспертов с криминологическим, юридическим или государственным опытом в области уголовного правосудия является необходимым, но ни в коем случае не достаточным условием для оправдания уважения к алгоритмической полицейской технологии.

Эти люди могут сами непреднамеренно выражать бессознательную предвзятость в своей работе или могут не распознавать подсознательные предубеждения или другие недостатки. Кроме того, их участие не устраняет риск того, что такая технология не обладает надежностью по причинам, выходящим за пределы их компетенции, или риск того, что правоохранительные органы используют технологию способом, который не соответствует закону о правах человека или Хартии. Таким образом, даже если независимые и квалифицированные эксперты с соответствующими знаниями предметной области были задействованы в разработке алгоритмической полицейской технологии, полное раскрытие использования технологии и всех соответствующих деталей должно происходить, чтобы обвиняемые в уголовном судопроизводстве могли оценить надёжность технологии, включая выявление любых неосознанных предубеждений или непреднамеренной дискриминации при разработке или использовании технологии, ведущих к потенциально незаконному ограничению свободы.

5.6.3. Заключительные комментарии: алгоритмическое соблюдение правил и право на надлежащую правовую процедуру

Уголовные суды в Канаде выполняют важную функцию контроля, включая оценку экспертных данных, таких как научные, психиатрические или судебные доказательства. Изучение этой роли ясно показывает, что суды должны иметь возможность получать значимое раскрытие информации о технологиях алгоритмической полицейской деятельности, их функциях, исходном коде, обучении и входных данных. Обеспечение такого раскрытия информации обеспечивает необходимую конституционную защиту, когда правоохранительные органы полагаются на технологию алгоритмического контроля в обстоятельствах, которые ограничивают или иным образом задействуют защищённые Хартией права человека, такие как право на свободу.

Кроме того, любые правоохранительные органы, которые рассматривают возможность внедрения технологий алгоритмического контроля, должны сначала убедиться, что право на надлежащую правовую процедуру не будет нарушено использованием таких технологий. Вопросы о надёжности, понятности и проверяемости таких технологий следует задавать – и получать ответы на них – с самого начала, до любых закупок или связанных с ними

государственных расходов на такие инструменты. Такие вопросы особенно необходимы, если технологии используются таким образом, чтобы воздействовать на реальных людей (т.е. приобретаются не только для целей внутренних пробных прогонов или моделирования, которые не имеют внешнего воздействия на жизнь и права любых людей или их сообществ). В тех случаях, когда правоохранительные органы полагались на технологию алгоритмического контроля для оправдания лишения кого-либо свободы, эта технология, помимо прочего, должна быть надёжной и беспристрастной.

В тех случаях, когда невозможно показать, что алгоритмический инструмент соответствует установленным требованиям, таким как, как минимум, надёжность и отсутствие предвзятости, инструмент не может разумно служить в качестве оправдания для лишения свободы в соответствии с принципами фундаментальной справедливости или другими соответствующими конституционными правами на надлежащую правовую процедуру.

В фокусе внимания № 8

Алгоритмические оценки воздействия

Эксперты по алгоритмической подотчётности в Соединенных Штатах предложили правительствам и государственным учреждениям использовать «алгоритмические оценки воздействия» (AIAs) для обеспечения прозрачности, подотчётности и соблюдения прав человека при развёртывании алгоритмических технологий.[1357] Включение требования AIAs на раннем этапе процесса рассмотрения любых технологий алгоритмического полицейского контроля предоставляет политикам основу для обдумывания и демонстрации общественности и независимым экспертам – потенциальных последствий использования такой технологии. Эта структура также предоставит возможность лицам, определяющим политику, разработать соответствующие механизмы для надзора и возмещения в случае, если технология всё ещё используется после завершения AIA. Правильно проведенная AIA будет включать в себя содержательные общественные консультации, которые позволят затронутым сообществам, внешним исследователям, экспертам по

[1357] See Andrew D Selbst, «Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109; and Dillon Reisman, Jason Schultz, Kate Crawford & Meredith Whittaker, «Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability" (April 2018) AI Now Institute. Selbst refers to «algorithmic impact statements" (AISs) in his paper; for ease of reference, this report uses «algorithmic impact assessments" to refer to both AIAs and AISs.

правам человека и гражданскому обществу понять, как используются технологии, выявить потенциальные проблемы и предоставить отзывы или рекомендации соответствующим органам, [1358] и бросить вызов предлагаемому или продолжающемуся использованию технологии, если это может нарушить конституционные права или права человека. [1359]Любая установленная структура AIAs для алгоритмических технологий полицейского контроля должна включать обязательства и процедуры для облегчения общественного обсуждения; внешняя проверка предлагаемых и текущих алгоритмических систем полицейского контроля; наращивание внутреннего институционального потенциала по вопросам, касающимся справедливости и неодинакового воздействия; надёжные механизмы надлежащей правовой процедуры для лиц или сообществ, подвергшихся негативному воздействию; а также определение и всесторонняя оценка всех разумных альтернативных решений для данной цели, включая альтернативу отказа от использования исследуемой технологии в общем. Дополнительные существенные компоненты должны включать требование к соответствующему государственному органу или правоохранительному органу: [1360]

- Раскрытие информации независимым экспертам, сообществам, которые исторически чрезмерно контролировались, и общественности предлагаемых и существующих алгоритмических технологий полицейского контроля, включая их цели, объём, работу, обучение и входные данные, а также соответствующие внутренние политики и юридические обязательства;
- Обозначение чистых выгод, которые технология, как ожидается, принесёт сообществам;
- Обозначение потенциальных вредных воздействий предлагаемых технологий, включая воздействия на права человека, социологические воздействия и материальные воздействия на местах;
- Использование для общественности и сообществ, которые могут быть затронуты, с особым акцентом на сообществах, которые исторически чрезмерно контролировались;
- Обрисовать в общих чертах стратегии смягчения каждого из выявленных потенциальных вредов;
- Обрисовать в общих чертах механизмы надзора и возмещения ущерба для оспаривания алгоритмических результатов или использования;

[1358] Andrew D Selbst, «Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 178-179.

[1359] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, «Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability", AI Now (April 2018), <https://ainowinstitute.org/aiareport2018.pdf> at 5.

[1360] При выполнении требований этих компонентов МАУ может ссылаться или включать отдельные обязательные обязательства по оценке воздействия, отчетности и публичной прозрачности, когда они налагаются, например, законодательными или обязательными директивами.

- Определить план обеспечения внешних исследователей, аудиторов, судов, комиссаров или следственных органов постоянным доступом для тщательной проверки предлагаемых технологий как до принятия, так и после, где это применимо.

Если технология алгоритмического полицейского контроля прошла AIA и была развернута, AIA следует регулярно обновлять на основе последней информации и исследований, включая информацию о влиянии технологии на затронутые сообщества.[1361]Процесс AIA также должен включать процедуры для заинтересованных сторон, чтобы оспорить конкретное агентство, если оно не выполняет требования AIA или любые последующие обязательства, вытекающие из AIA. [1362]

1 апреля 2019 года Казначейский совет секретариата Канады («Казначейский совет») ввел в действие обязательную Директиву об автоматизированном принятии решений («Директива»). Среди других требований, таких как тестирование системы перед развёртыванием, Директива требует, чтобы федеральные правительственные ведомства проводили предписанный AIA перед вводом в «производственную среду» (т.е. развёртывание вне внутренней тестовой среды) любой автоматизированной технологии принятия решений, которая предназначена для дополнения или заменить суждения людей, принимающих решения. [1363] Чтобы облегчить этот процесс, Казначейство предоставляет онлайн-инструмент под названием «Оценка алгоритмического воздействия», который представляет собой анкету, предназначенную для помощи федеральным ведомствам в проведении внутренней оценки и снижения рисков, связанных с использованием алгоритмических методов. [1364]

Вначале важно отметить, что Директива совета казначейства не включает особого внимания к использованию алгоритмической технологии в системе уголовного правосудия, поэтому в ней могут отсутствовать соображения, соответствующие этому контексту. Директива также не применяется за пределами федеральных учреждений, однако, как показано в этом отчёте, многие алгоритмические технологии полицейской деятельности приняты и внедрены на провинциальном или муниципальном уровне. Поскольку принятие аналогичной Директивы для провинций или муниципалитетов находится за

[1361] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, «Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability", AI Now (April 2018), <https://ainowinstitute.org/aiareport2018.pdf> at 10.

[1362] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, «Algorithmic Impact Assessments: A Practical Framework Public Agency Accountability", AI Now (April 2018), <https://ainowinstitute.org/aiareport2018.pdf> at 10.

[1363] Government of Canada, «Directive on Automated Decision-Making", <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

[1364] «Algorithmic Impact Assessment" (29 March 2019) Government of Canada <https://open.canada.ca/aia-eia-js/?lang=en

пределами юрисдикции Совета казначейства, в этом отчёте рекомендуется, чтобы провинции и территории вводили в действие свои собственные директивы и требования AIA с надёжными механизмами прозрачности, подотчётности и надзора там, где провинциальные или муниципальные государственные органы, такие как правоохранительные органы и полицейские службы, рассматривали возможность внедрения алгоритмических технологий принятия решений.

Из-за ограничений, предоставленный Казначейством инструмент оценки воздействия (далее именуемый «вопросник») содержит серьёзные недостатки, которые не позволяют ему быть эффективным инструментом надзора, прозрачности или подотчётности. Анкета очень далека от того, что было сформулировано исследователями, такими как Селбст и специалистами AI Now Institute, как составляющие AIA, иона не соответствует общему пониманию подобных видов оценок воздействия, таких как конфиденциальность оценки воздействия (PIA), которые уже требуются в других контекстах в Канаде. [1365] По оценкам, заполнение анкеты займет 35 минут и содержит около 60 вопросов, [1366] почти все из которых имеют формат множественного выбора или ответы на них даны на основе «да/нет». Анкета не требует предоставления подтверждающих деталей или документации для обоснования ответов в отношении потенциальных воздействий, мер по снижению рисков или объяснений того, как предлагаемая программа работает как на техническом, так и на операционном уровне. [1367] Более того, анкета Казначейства не определяет, что представляют собой «высокие» или «низкие» риски, воздействия или ставки для затронутых или уязвимых сообществ. Он полагается на то, что респонденты сами оценят или предоставят соответствующий опыт, чтобы дать ответы, которые приведут к точной оценке.

[1365] Оценка воздействия на частную жизнь (ДИП) представляет собой "процесс управления рисками, который помогает учреждениям обеспечивать соответствие законодательным требованиям и определять влияние их программ и мероприятий на частную жизнь людей". Завершение ДИП в данных обстоятельствах является юридическим обязательством в соответствии с различными канадскими законами о неприкосновенности частной жизни, такими, как федеральный закон о неприкосновенности частной жизни, законодательство различных учреждений или государственная политика и директивы. Expectations: OPC's

[1366] Ibid.

[1367] В отличие от этого, проект оценки воздействия на конфиденциальность, который Полицейская служба Калгари провела при принятии продуктов и услуг Palantir в 2014 году, насчитывает почти пятьдесят страниц существенных подробностей и анализа, касающихся технологии, ее внедрения и связанных с ней правовых и политических вопросов только для защиты конфиденциальности и данных. Calgary Police Service, "Калгари Police Service Palantir Implementation Privacy Impact Assessment: 1 июня 2014 Черновик" 29-30, (получен посредством запроса свободы информации 18-G-1921). Для дальнейшего контекста, проводя различие между другими формами оценки воздействия в Соединенных Штатах, такими как "заявления о расовом воздействии" и отчеты о воздействии наблюдения, Селбст отмечает: "Хотя существует ценность прозрачности, которую обеспечивают эти документы, эти версии заявлений о воздействии не столь надежны, как предлагаемая АИС [утверждение об алгоритмическом воздействии]. На них может быть всего лишь несколько страниц, в то время как правила требовались для ограничения EIS [заявлений о воздействии на окружающую среду, на которых основывались AIA] 150 страницами, за исключением случаев "необычного охвата или сложности", которые предоставляются 300 ". Andrew D Selbst, «Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 186.

В то время как анкета Казначейского совета может служить полезным инструментом предварительной внутренней оценки для проверки идей перед инвестированием в них дополнительных ресурсов, этот инструмент в его нынешней форме не будет выполнять функцию того, что обычно считалось значимой AIA, например, предлагаемой Зельбст и AI Now Institute. Любая AIA, принятая в Канаде, должна следовать последней модели, которая, соответственно, потребовала бы большего количества государственных органов или правоохранительных органов, которые хотели бы использовать технологии алгоритмического контроля над представителями общественности.

Право на средство правовой защиты

Право на средство правовой защиты, как это предусмотрено ICCPR, и гарантиями того, что те, чьи права человека или конституционные права были нарушены, могут получить существенное возмещение за такие нарушения.[1368] ICCPR требует от подписавших его государств обеспечить, чтобы «любое лицо, права или свободы которого (установленные в ICCPR) нарушены, имело эффективное средство правовой защиты»; что любые требования о средствах правовой защиты должны «определяться компетентными судебными, административными или законодательными органами»; и что компетентные органы должны применять любые предоставленные средства правовой защиты.[1369] Хартия предоставляет аналогичную гарантию в разделе 24 (1): «Любой, чьи права или свободы, гарантированные настоящей Хартией, были нарушены или им отказано, может обратиться в суд компетентной юрисдикции для получения такого средства правовой защиты, которое суд сочтёт целесообразным и справедливым. в сложившихся обстоятельствах».[1370] В контексте уголовного правосудия раздел 24 (2) предусматривает конкретное средство правовой защиты, согласно которому доказательства могут быть исключены из допустимых в некоторых случаях, если они были получены

[1368] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 2.3; Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 24. See also, UN General Assembly, «Resolution adopted by the General Assembly on 16 December 2005: Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law", (21 March 2006) <https://www.ohchr.org/EN/ ProfessionalInterest/Pages/RemedyAndReparation.aspx>.

[1369] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/ pages/ccpr.aspx>, art 2.3.

[1370] Canadian Charter of Rights and Freedoms, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 24(1).

способом, который «нарушал или отрицал» какие-либо права или свободы, закрепленные в Хартии.[1371]

Технологии алгоритмического контроля создают множество осложнений для возможности пострадавшего человека реализовать своё право на эффективное средство правовой защиты. Специальный докладчик ООН по защите и поощрению свободы выражения мнений и Верховный комиссар по правам человека признали, что алгоритмические системы и нарушения конфиденциальности в результате наблюдения создают особые проблемы в этом отношении,[1372] которые будут рассмотрены в следующих подразделах. В разделе 5.7.1 анализируется отсутствие в законодательстве Канады требования об уведомлении правоохранительных органов об общем или конкретном наблюдении, включая алгоритмическое наблюдение. В нем также обсуждается, как отсутствие уведомления влияет на способность оспаривать использование алгоритмической полицейской технологии там, где оно нарушает конституционное право или право человека. В разделе 5.7.2 обсуждается, что означает эффективное средство правовой защиты и почему использование судебных разбирательств для исправления нарушений конституции или прав человека с помощью алгоритмической работы полиции может быть недостаточной защитой.

1.1.1 Требования к уведомлению и возможность оспорить алгоритмическую политику

Международные эксперты по правам человека выразили обеспокоенность по поводу отсутствия уведомления лиц, права которых могли быть затронуты алгоритмической обработкой, и по поводу этого вмешательства в их право на средство правовой защиты.[1373] Верховный комиссар ООН по правам человека заявил, что уведомление об общих или конкретных мерах наблюдения (обычно ex post facto или уведомление, предоставляемое после факта) и обеспечение того, чтобы пострадавшие лица имели законное право оспаривать эти меры, являются «критическими вопросами при определении доступа к эффективному средству правовой защиты».[1374] В настоящее время канадские

[1371] Ibid, s 24(2).
[1372] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> para 40; UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 54.
[1373] UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40.
[1374] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 40; UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for

правоохранительные органы обязаны уведомлять лиц, которые были объектом электронного наблюдения, путём перехвата частных сообщений.[1375] При рассмотрении требования об уведомлении о слежке за прослушиванием телефонных разговоров Верховный суд Канады подтвердил, что «право на неприкосновенность частной жизни подразумевает не только свободу от необоснованного обыска и изъятия, но и возможность выявлять такие вторжения и оспаривать их, а также искать действенные средства правовой защиты. Уведомление усиливает все эти интересы».[1376] Уведомление, таким образом, является средством облегчения значимого доступа к средствам правовой защиты от нарушений Устава и прав человека, совершенных данным правоохранительным органом. Несмотря на это признание важности уведомления, внутренние законы о конфиденциальности обычно освобождают правоохранительные органы от требований уведомлять людей о деятельности по сбору данных вне контекста наблюдения за прослушиванием телефонных разговоров.[1377] Эти исключения могут включать сбор данных с помощью технологий алгоритмического контроля, и объём правовой обязанности по уведомлению объектов электронного наблюдения не был полностью определён, поскольку суды ещё не рассмотрели этот вопрос внимательно. Таким образом, может существовать фундаментальный раскол между тем, что требует закон о правах человека, и тем, что фактически предоставляется или не предоставляется отдельным лицам посредством практики канадских правоохранительных органов и системы уголовного правосудия.

Важность уведомления отдельных лиц и общественности о том, как правоохранительные органы проводят технологическое наблюдение, усиливается еще большей важностью раскрытия информации обвиняемым. Получив уведомление, обвиняемые в уголовных судах могут предпринять шаги для обеспечения получения всех прав, другой информации, необходимой для полноценного ответа и защиты.

Однако требование об уведомлении также важно для лиц, которые столкнулись с потенциальными нарушениями конфиденциальности или свободой выражения, или дискриминацией, но, если Корона не предъявила

Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 41 and 54.

[1375] Criminal Code, s 196.

[1376] R v Tse, 2012 SCC 16 at para 83.

[1377] См. Закон о свободе информации и защите частной жизни, RSBC 1996, c 165, s 27 (3) a); Закон о свободе информации и защите частной жизни, RSO 1990, c F.31, s.39 (3); Муниципальный закон о свободе информации и защите частной жизни, RSO 1990, c M.56, s. 29 (3) a), в котором содержатся четкие исключения из общего требования об уведомлении в отношении личных данных, собираемых для целей правоприменения. В других законодательных актах, касающихся неприкосновенности частной жизни, таких, как Закон о неприкосновенности частной жизни и Закон Альберты об охране частной жизни, положения об изъятиях, допускаемых правоохранительными органами, содержат положения, согласно которым уведомление не требуется, если его предоставление может привести к сбору недостоверных данных (см. Закон о неприкосновенности частной жизни, RSC 1985, c P-21, s5 (3); Закон о свободе информации и защите частной жизни, RSA 2000, c F-25, 34 (3).

уголовных обвинений после совершения действий, которые привели к таким нарушениям. Например, если люди ошибочно идентифицируются системами распознавания лиц, такими как те, которые используются Полицейской службой Калгари и Полицейской службой Торонто, документы CPS и TPS, выпущенные по запросам FOI, не указывают, что эти люди будут уведомлены.[1378]Лица, изображения которых фиксируются с помощью технологии распознавания лиц, могут пострадать от ряда нарушений гражданских свобод, включая вред, связанный с задержанием или арестом, или вторжения в частную жизнь, вызванные другими методами полицейского расследования (например, обыски в доме человека, доступ к личному содержимому конфискованного компьютера или обыск с полным арестом). Такой вред может возникнуть даже в том случае, если последующее расследование в конечном итоге не приведёт к возбуждению уголовного дела. Кроме того, необоснованные нарушения гражданских свобод наносят индивидуальный и общественный ущерб основным свободам, которые защищены конституционными гарантиями неприкосновенности частной жизни и свободы слова. Именно по этой причине гражданские убытки за нарушения Устава предназначены для обеспечения компенсации, оправдания и предотвращения подобных нарушений в будущем.[1379] Оправдание «как объект конституционного ущерба фокусируется на вреде, который нарушение Хартии причиняет государству и обществу».[1380] Точно так же люди, которые могут быть пойманы алгоритмами наблюдения в социальных сетях на основе их общения, связей или местоположения, могут хранить свои данные в правоохранительных системах без их ведома.[1381]Тем не менее, канадские правоохранительные органы исторически не предоставляли такое уведомление при мониторинге онлайн или офлайн-активности протестующих.[1382] Короче

[1378] Mark Saunders, «Facial Recognition System", 17 May 2019, pages 2-3, presented at meeting of Toronto Police Services Board, 30 May 2019; Calgary Police Service, «Facial Recognition Technology, Ref #IN-006-1" (obtained through freedom of information request 18-G-1921); and Calgary Police Service, «Facial Recognition 2018" (obtained through freedom of information request 18-G-1921).

[1379] Ванкувер (город) против района, 2010 SCC 27. В гражданских исках о возмещении ущерба в связи с нарушениями Хартии суды уполномочены возмещать ущерб в целях личной компенсации, оправдания или сдерживания. Личные убытки не являются исключительно предметом внимания. В рамках личной компенсации основное внимание уделяется личным потерям заявителя (физическим, психологическим и материальным), а также нематериальному ущербу заявителя, такому, как бедствие, унижение, смущение и беспокойство.

[1380] Vancouver (City) v Ward, 2010 SCC 27 at para 28.

[1381] См. раздел 5.3 ("Права на свободу выражения мнений, мирные собрания и ассоциации"), в котором обсуждается растущее количество эмпирических данных, проливающих свет на проблемную связь между правительственным онлайн-наблюдением, включая простую перспективу такого наблюдения, и такими леденящими последствиями для свободы выражения мнений.

[1382] Например, Полицейская служба Торонто и КККП следят за протестующими чернокожими и коренными народами, которые стали известны общественности лишь после обнародования документов в ответ на просьбы о свободе информации: Marilyn Robak, «'We've always been seen as a threat,' says former N.W.T. premier of RCMP surveillance revelations", CBC News (20 November 2016) <https://www.cbc.ca/news/canada/north/indigenous-trust-reconciliation-mmiw-protesters-rcmp-surveillance-1.3857009>; Stephen Davis, «Police monitored Black Lives Matter Toronto protesters in 2016, documents show", CBC News (3 May 2018) <https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628>.

говоря, хотя существенный вред конституционным правам человека может быть нанесён прямо или косвенно в результате применения алгоритмической полицейской технологии, в настоящее время в канадском законодательстве нет гарантии уведомления отдельных лиц, когда они подвергаются воздействию такой технологии, и, следовательно, не является гарантией того, что они смогут получить средства правовой защиты от связанных нарушений. Требование уведомления напрямую связано со способностью реализовать право на эффективное средство правовой защиты. Чтобы получить доступ к средству правовой защиты, пострадавшие лица должны действительно осознавать, что изолируется.

Это непростой вопрос, когда дело доходит до технологии алгоритмического контроля, потому что люди могут даже не знать, что они были объектом алгоритмического наблюдения или прогнозов.[1383] Например, в Новом Орлеане лица, обвиненные в принадлежности к банде на основе анализа данных, управляемого Palantir, не были проинформированы об использовании программного обеспечения в их уголовных процессах.[1384] Уведомление также может быть затруднено с точки зрения логистики в некоторых обстоятельствах, когда алгоритмический инструмент используется для сбора больших объёмов информации о многих лицах. Однако отдельные лица (и их юрисконсульт) не могут оспаривать алгоритмические решения или выводы о них, если они не осведомлены о таких решениях или выводах, не говоря уже о том, чтобы подавать юридические вызовы самим инструментам алгоритмического контроля.

Даже в тех случаях, когда люди знают, что они стали мишенью алгоритмического контроля, проблема чёрного ящика представляет собой дополнительный информационный барьер для доступа к эффективным средствам защиты.[1385] Если физические лица и их законные представители не могут понять, как действует система, нацеленная на них, они могут не понимать, как были нарушены их права. Кроме того, право на средство правовой защиты подвергается неблагоприятному воздействию, если люди не могут изучить технологии алгоритмического контроля, которые затронули их, и, таким образом, оспорить точность, надёжность и справедливость тех технологий, которые потенциально нарушили их права человека, будь то по

[1383] Совет ООН по правам человека, "Право на неприкосновенность частной жизни в цифровую эпоху: доклад Верховного комиссара ООН по правам человека" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 54; UN General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40.

[1384] Ali Winston, «New Orleans ends its Palantir predictive policing program", The Verge (15 March 2018) <https://www.theverge. com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end>.

[1385] См. вышеприведенные обсуждения алгоритмической прозрачности и проблемы черного ящика, а также пример State v Loomis в разделе 5.6.1 ("Информационные барьеры на пути к должной процедуре: алгоритмическая прозрачность и влияние частного сектора").

причине понятности или коммерческого сопротивления и попытки оградить проприетарное программное обеспечение от проверки.[1386]

Средства правовой защиты от нарушений прав человека должны быть эффективными

Эффективные средства правовой защиты должны быть известны и доступны лицам, права которых были нарушены.[1387] Чтобы быть эффективными, средства правовой защиты должны быть способны положить конец продолжающимся нарушениям прав. Более того, государства должны принимать меры для предотвращения повторения нарушений прав.[1388] Например, средства правовой защиты должны включать в себя возможность суда приказать правоохранительному органу прекратить использование определённого инструмента или категории инструментов алгоритмического контроля. UB в соответствии с Хартией право на средство правовой защиты потенциально может привлечь внимание суда к широко распространенной или систематической практике в отношении нарушений Хартии в каждом отдельном случае.[1389] Учитывая, что технологии алгоритмического контроля могут иметь воздействие на уровне сообщества, важна потребность в средствах правовой защиты, которые должны быть достаточно значимыми и реагировать на истинный масштаб и влияние нарушения.

Например, в некоторых делах статьи 8 (включая право не подвергаться необоснованному обыску и изъятию) суды признали важность защиты прав на неприкосновенность частной жизни третьих лиц, которые не являются ответчиками в суде.[1390] Первоначально Верховный суд Канады постановил, что степень вторжения в частную жизнь с участием третьих лиц имела значение только в обстоятельствах, связанных с «потенциально массовым вторжением в ... частную жизнь» представителей общественности, которые не были

[1386] UN Human Rights Council, «The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 55.

[1387] UN Human Rights Council, «The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, para 40.

[1388] UNHRC, General Comment No 31 [80] (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant), 80th Sess, adopted 29 March 2004, CCPR/C/21/Rev1/Add13, at paras 15, 17, 19 <https://digitallibrary.un.org/record/533996?ln=en>.

[1389] См. R v Rogers Communications, 2016 ONSC 70. Однако способность отдельных сторон в споре поднимать вопрос о нарушениях Хартии прав третьих сторон по-прежнему меняется и остается несколько неопределенной.

[1390] См. R v Marakah, [2017] 2 SCR 608; R. v Thompson, [1990] 2 SCR 111 (где SCC постановил, что перехват с телефона общего пользования привел к нарушению прав на неприкосновенность частной жизни третьей стороны, что сделало перехват прослушки правоохранительными органами необоснованным и нарушающим статью 8); R v Mahmood, [2008] OJ No 3922 (SCJ), additional reasons [2009] OJ No 319, and later on appeal, 2011 ONCA 693 (where the court considered and found section 8 violations occurring due to a tower dump production order's sheer breadth and scope); R v Guindon, 2015 ONSC 4317.

причастны к предполагаемой преступной деятельности».[1391] Однако эта позиция была расширена в 2017 году, когда неконституционный обыск мобильного телефона другого лица был конституционно значим для утверждения ответчика о нарушении его собственного права, предусмотренного статьей 8. Нарушение третьей стороной имело отношение к средству правовой защиты ответчика, которое требовало исключения полученных доказательств.[1392] Такое обоснование может относиться к лицам, права которых или права третьих лиц на конфиденциальность были нарушены, например, с помощью распознавания лиц или алгоритмического анализа социальных сетей. Таким образом, в Канаде эффективное право на средство правовой защиты от нарушений конституции или прав человека с использованием технологий алгоритмического контроля может потребовать признания того факта, что нарушение права третьей стороны на неприкосновенность частной жизни посредством использования этих технологий может сделать поиск неконституционным в соответствии с разделом 8 Устава в случае данного ответчика. Несмотря на судебные решения, которые на сегодняшний день предоставляют одну из форм защиты от незаконного наблюдения в уголовных делах, ответственность за неправомерное использование интрузивных технологий может быть неуловимой, если надзор в основном возникает только в ходе судебного разбирательства. Отдельные стороны в судебном процессе могут не обеспечить достаточной проверки систематической практики массового наблюдения. Регуляторный и судебный надзор на перспективной и постоянной основе (например, с помощью ордеров, требований к отчётности и законов, устанавливающих ограничения и гарантии использования технологий алгоритмического контроля) может обеспечить необходимые сдержки и противовесы, предполагая, что рассматриваемый алгоритмический инструмент может быть используются в соответствии с Хартией и обязательствами правоохранительных органов в области прав человека. Однако гарантии должны быть тщательно разграничены на том основании, что слишком широкие стандарты или правила могут просто функционировать как средство бессмысленных гарантий «соблюдения» без обеспечения подлинной или существенной защиты охраняемых Хартией и международных прав человека.

[1391] R v Edwards, [1996] 1 SCR 128 at para 38; R v Thompson, [1990] 2 SCR 1111 at 1143.
[1392] R v Marakah, [2017] 2 SCR 608.

Заключительные комментарии: алгоритмическое наблюдение и право на средство правовой защиты

В свете многих конституционных проблем и проблем, связанных с правами человека, которые освещены в части 5 («Последствия алгоритмической полицейской деятельности в соответствии с международными правами человека и Хартией для прав человека»), важно, чтобы люди имели доступ к эффективным средствам правовой защиты от потенциальных нарушений прав, вызванных алгоритмической технологией.

Однако эти технологии создают проблемы, поскольку их функционирование и использование обычно затрудняется секретностью и проблемами чёрного ящика. Без доступа к информации люди не могут реализовать своё право на средство правовой защиты. Следовательно, у них не будет критически важного средства компенсации вредного воздействия этих технологий, которое потенциально могло бы остаться полностью или в значительной степени неконтролируемым, тем самым воспроизводя историческую несправедливость, которая может возникнуть из-за предвзятых методов или систем полицейской деятельности.

Подход к алгоритмической деятельности полиции, основанной на соблюдении прав человека

В части 5 этого отчёта содержится специальный правовой и политический анализ потенциальных последствий алгоритмических полицейских технологий для каждого из нескольких основных прав человека, защищённых международным и внутренним законодательством о правах человека и Канадской хартией. В частности, использование технологий алгоритмического контроля правоохранительными органами вводит или усугубляет риски нарушения права на неприкосновенность частной жизни (раздел 5.2); права на свободу выражения мнений, мирных собраний и ассоциаций (раздел 5.3); право на равенство и свободу от дискриминации (раздел 5.4); право на свободу и свободу от произвольного задержания (раздел 5.5); право на надлежащую правовую процедуру (раздел 5.6); и право на средство правовой защиты (раздел 5.7). Выводы и заключения о том, как алгоритмические полицейские технологии влияют на каждое из этих прав человека, были резюмированы в соответствующих разделах выше и повторяются в соответствующих разделах следующей части этого отчета, (часть 6 «Рекомендации и заключение»).

Часть 6 основана на правовом и политическом анализе, содержащемся в части 5 отчёта, синтезированном с фактическими выводами о текущем состоянии алгоритмической полицейской деятельности в Канаде в части 4 («Алгоритмическая полицейская деятельность в Канаде: текущая ситуация»), чтобы предоставить набор рекомендаций правительству Канады, правоохранительным органам и другим участникам системы уголовного правосудия. Каждая рекомендация вытекает непосредственно из исследований и анализа, проведённых в этом отчёте; однако некоторые рекомендации могут содержать новую информацию, которая требуется для более полного обоснования того, как такая рекомендация может быть выполнена. В совокупности эти рекомендации обеспечивают всеобъемлющую, хотя и не исчерпывающую основу для поддержки правовой и политической реформы с целью смягчения или предотвращения негативного воздействия использования правоохранительными органами алгоритмических полицейских технологий на конституционные права и права человека, особенно тех, которые принадлежат к исторически маргинализированным сообществам, которые пострадают больше всего.

Рекомендации и заключение

Этот отчёт выявил ряд серьёзных недостатков в политике, практике и законодательстве, связанных с использованием технологий алгоритмической полицейской деятельности в Канаде. Результаты исследования в части 4 («Алгоритмическая полицейская деятельность в Канаде: текущая ситуация») описывают, как несколько правоохранительных органов по всей стране используют или разрабатывают различные формы алгоритмических полицейских технологий. В сопроводительном правовом анализе в части 5 («Последствия алгоритмической полицейской деятельности для международных прав человека и Хартии прав человека») обсуждается, как такие технологии обладают высоким потенциалом нарушения основных прав и свобод человека, которые защищены Конституцией и международным правом прав человека. В части 6 обобщены эти недостатки и представлены рекомендации для обеспечения того, чтобы правоохранительные органы и правительства соблюдали конституционные права и права человека всякий раз, когда они рассматривают возможность разработки или внедрения технологий алгоритмической полицейской деятельности. Эти рекомендации также следует рассматривать как применимые задним числом к технологиям алгоритмической полицейской деятельности, которые были разработаны, приняты или иным образом уже используются канадскими правоохранительными органами.

Ключевым вдохновляющим принципом, лежащим в основе рекомендаций, является потребность в надёжных стандартах прозрачности и подотчётности. В процессе подготовки данного отчёта возник ряд общих препятствий, которые продемонстрировали значительную информационную асимметрию между правоохранительными органами и общественностью. Помимо барьеров в канадских процессах свободы информации (FOI), как описано в разделе 4.4 («Ограничения результатов исследований»), некоторые правоохранительные органы воздерживаются от публичного раскрытия информации об их использовании или внедрении технологий алгоритмического контроля. Это нежелание включало отказ от раскрытия того, какие агентства используют определённые типы алгоритмических технологий полицейского контроля, включая конкретные коммерческие продукты, а также отказ проактивно объяснить, как такая технология используется. Отсутствие полной информации представляет собой серьёзную проблему при определении степени, в которой существующее или потенциальное использование технологий алгоритмической полицейской деятельности может нарушать конституционные обязательства полицейских органов и права человека или может вызывать другие юридические проблемы. В результате многие из рекомендаций данного отчёта сосредоточены на установлении требований прозрачности как необходимого предварительного условия для общественной подотчётности. Необходимы сильные механизмы подотчётности, чтобы лица, определяющие политику, и общественность могли осмысленно продумывать и определять риски и вред конституционным правам и правам человека, которые возникают в результате разработки или использования любых заданных алгоритмических полицейских технологий, до того, как произойдет такая разработка или использование. В случае принятия взвешенного решения о внедрении алгоритмической технологии полицейского контроля необходимы механизмы подотчётности для установления ограничений и мер, необходимых для защиты конституционных прав и прав человека при каждом использовании этого конкретного инструмента.

В дополнение к требованиям прозрачности и подотчётности, рекомендации в этом отчёте вдохновлены необходимостью ввести общенациональный мораторий на все алгоритмические полицейские технологии до тех пор, пока не будет проведено полное расследование этого класса технологий и не будут введены конституционные гарантии. Такие моратории необходимы для смягчения вреда от неизученного использования алгоритмической полицейской технологии и для обеспечения того, чтобы технология не выходила за рамки прав человека и закона, когда дело доходит до уголовного правосудия. Что касается введения таких мораториев, в Канаде имеется сложная сеть регулирующих субъектов, которые разделяют частично

совпадающие роли в управлении и надзоре за законодательством правоохранительных органов.

Правила различаются в зависимости от провинции, в которой расположена любая данная полицейская служба, и от классификации службы как муниципальной, провинциальной /территориальной/региональной (все они упоминаются в части 6 как «провинциальные») или федеральной. Например, как муниципальные, так и провинциальные правительства могут регулировать работу муниципальных полицейских служб путём введения моратория на использование определённых технологий. В результате все уровни правительства, обладающие юридическими полномочиями в отношении правоохранительных органов, могут и должны установить как немедленные временные остановки (например, моратории), так и, в ожидании дальнейшего изучения и оценки воздействия, долгосрочные ограничения или полные запреты на использование определённых алгоритмических полицейских технологий.

В части 6 представлено в общей сложности двадцать рекомендаций по защите прав человека в контексте алгоритмической работы полиции. Среди них авторы данного отчёта определили набор из семи приоритетных рекомендаций, которые правительства и правоохранительные органы должны предпринять в срочном порядке. Эти рекомендации, если они будут реализованы, с наибольшей вероятностью уменьшат наиболее серьёзные нарушения прав человека и Хартии, которые могут произойти в результате использования канадским правительством и правоохранительными органами технологий алгоритмической полицейской деятельности.

Приоритетные рекомендации для алгоритмической работы полиции в Канаде:

1. Правительства должны ввести мораторий на использование правоохранительными органами технологий, основанных на алгоритмической обработке исторических массивов полицейских данных, в ожидании завершения всесторонней проверки посредством судебного расследования, а также на использование алгоритмической полицейской технологии, которая не отвечает предварительным условиям надёжности, необходимости и соразмерности.

2. Федеральное правительство должно провести всесторонний анализ возможностей использования правоохранительными органами

исторических наборов полицейских данных для использования в технологиях алгоритмической полицейской деятельности.

3. Правительства должны создать условия надёжности, необходимости и соразмерности, необходимые для использования алгоритмических полицейских технологий, и ввести мораторий на каждую алгоритмическую полицейскую технологию, которая не соответствует этим установленным предпосылкам.

4. Правоохранительные органы должны быть полностью прозрачными для общественности и с уполномоченными по вопросам конфиденциальности, незамедлительно раскрывая, используются ли, разрабатываются или закупаются в настоящее время алгоритмические полицейские технологии, чтобы обеспечить демократический диалог и значимую подотчётность, и надзор.

5. Правительствам провинций следует принять директивы, касающиеся использования и закупки технологий алгоритмического контроля, включая требования о том, что правоохранительные органы должны проводить алгоритмические оценки воздействия до разработки или использования любых технологий алгоритмического контроля; публиковать ежегодные общедоступные отчёты, раскрывающие подробности использования технологий алгоритмического контроля, включая информацию о любых связанных данных, таких как источники обучающих данных, потенциальные смещения данных, а также входные и выходные данные, где это применимо; и публиковать независимые экспертные обзоры и научное подтверждение любой такой технологии перед использованием.

6. Правоохранительные органы не должны бесконтрольно использовать технологии алгоритмического наблюдения в общественных местах: полицейские службы должны запрещать использование алгоритмических прогнозов для оправдания вмешательства в личную свободу и должны получать предварительное судебное разрешение перед развертыванием инструментов алгоритмического наблюдения на публичных собраниях и в онлайн-средах.

7. Правительства и правоохранительные органы должны привлекать внешних экспертов, в том числе специалистов из исторически маргинализированных сообществ, на которые непропорционально сильно влияет система уголовного правосудия, при разработке механизмов регулирования и надзора для алгоритмических полицейских технологий, в рамках выполнения алгоритмических оценок воздействия и мониторинга последствий алгоритмических технологий полицейского контроля, которые были введены в действие.

Каждая из этих приоритетных рекомендаций разработана и более подробно объясняется ниже, где они представлены в полном наборе рекомендаций. Полный набор, представленный в разделах с 6.1 по 6.5, следует структуре юридического анализа в части 5 и разбит на категории по каждому обсуждаемому праву человека: право на неприкосновенность частной жизни (раздел 6.1); права на свободу выражения мнений, мирных собраний и ассоциаций (раздел 6.2); право на равенство и свободу от дискриминации (раздел 6.3); право на свободу (раздел 6.4); и права на надлежащую правовую процедуру и средства правовой защиты с упором на подотчётность и прозрачность (раздел 6.5). Раздел 6.6 содержит заключительные комментарии ко всему отчёту. Каждый раздел содержит рекомендации, которые имеют высший приоритет и должны рассматриваться как пороговые вопросы при рассмотрении любой конкретной технологии алгоритмического контроля. Эти рекомендации по пороговым значениям, которые частично совпадают с рекомендациями по приоритетам, имеют гораздо большее значение, чем другие, и должны рассматриваться в первую очередь, потому что, если их принять во внимание, рекомендации по пороговым значениям могут привести к запретам или серьёзным ограничениям на некоторые формы или способы использования технологии алгоритмического контроля. Ничто меньшее не может в достаточной степени защитить конституционные права или права человека. В этом контексте последующие рекомендации становятся спорными, неприменимыми или менее важными, поскольку они вступают в силу только в том случае, если технология алгоритмического контроля фактически используется.

В качестве руководства рекомендации имеют цветовую кодировку в зависимости от того, являются ли они рекомендацией порогового значения приоритета или дополнительной рекомендацией, которая будет применяться только в том случае, если технология алгоритмического контроля ещё не была ограничена мораториями, запретами или другими значительными юридическими ограничениями, препятствующими ее использованию:

ПРИОРИТЕТНЫЕ РЕКОМЕНДАЦИИ: это рекомендации по приоритетным пороговым значениям, которые правительства и правоохранительные органы должны задействовать сейчас, чтобы смягчить некоторые из наиболее серьёзных нарушений прав человека и Хартии, которые могут произойти в результате использования правительством и правоохранительными органами Канады технологий алгоритмического контроля.

ДОПОЛНИТЕЛЬНЫЕ РЕКОМЕНДАЦИИ: это рекомендации, которые станут применимыми и важными в обстоятельствах, когда технология алгоритмического контроля не запрещена человеческими и конституционными

правами, не заблокирована или ограничена мораториями и ограничениями, изложенными в приоритетных рекомендациях.

6.1. Рекомендации по защите права на неприкосновенность частной жизни

Технологии алгоритмического контроля реализуют право на неприкосновенность частной жизни в результате методов сбора, обработки и обмена данными, на которые обычно полагаются такие технологии, а также из-за проблем с точностью данных, которые часто возникают с этими технологиями. Эти инструменты контроля обычно обрабатывают большие наборы данных, чтобы попытаться спрогнозировать или раскрыть информацию, или сделать выводы, которые затем могут быть приняты правоохранительными органами. Должны быть разработаны или поддержаны правовые гарантии или конституционная защита, чтобы люди сохраняли возможность быть полностью свободными от необоснованного вмешательства в частную жизнь и гарантировать, что защищенные зоны конфиденциальности не будут разрушены расширением методов сбора данных и возможностей алгоритмического наблюдения. Определение соответствующих защитных мер – не всегда простая задача. Технологии алгоритмического контроля могут бросить вызов существующим конституционным гарантиям и гарантиям прав человека там, где правовая система ещё не имела возможности создать четкий набор правил, которым должны следовать правоохранительные органы, но где потребность в защите частной жизни становится большой. Это включает агрегирование данных, которые были «извлечены» из Интернета, или использование биометрических данных, которые могут быть получены без согласия человека. Кроме того, алгоритмические технологии полицейского контроля создают новые проблемы с конфиденциальностью за счёт нового использования старых данных (т.е. перепрофилирования полицейских данных), которые были собраны правоохранительными органами задолго до того, как были рассмотрены алгоритмические методы полицейского контроля. Существующие правовые средства защиты этих типов данных, такие как базы данных с фотографиями, могут быть недостаточными в свете расширенных возможностей алгоритмической обработки.

Авторы предлагают семь рекомендаций для решения возможных проблем конфиденциальности, связанных с технологиями алгоритмического контроля. Эти рекомендации, как правило, сосредоточены на том, чтобы требовать от всех технологий алгоритмического контроля соблюдения предварительных условий необходимости, пропорциональности и надёжности, прежде чем они могут быть использованы; о механизмах надзора; о важности точности данных.

Рекомендация 1: Правительства должны создать предпосылки надёжности, необходимости и соразмерности при использовании алгоритмической полицейской технологии.

Муниципальные, провинциальные и федеральные правительства в той мере, в какой они контролируют полицейские службы в Канаде, должны ввести моратории на все технологии алгоритмического наблюдения, которые не соответствуют пороговым требованиям надёжности, необходимости и соразмерности. Мораторий должен немедленно начаться с технологии распознавания лиц. Все алгоритмические технологии полицейского контроля должны пройти оценку, чтобы определить, является ли технология надёжной; необходимо ли использование технологии правоохранительными органами для выполняемых задач и их заявленных целей; соразмерна ли технология задачам и целям с учётом связанных затрат, рисков и вреда. В некоторых обстоятельствах использование технологии алгоритмического контроля может быть недостаточно надёжным, чтобы оправдать использование; может быть необязательным с учётом разумных альтернатив (включая альтернативу неприменения предлагаемой технологии для заявленной цели); или может непропорционально нанести ущерб конфиденциальности. Например, технология распознавания лиц, основанная на большом количестве изображений, извлечённых из Интернета, скорее всего, будет несовместима с фундаментальными нормами конфиденциальности. Как показывает растущее количество исследований, опасность этого алгоритмического метода наблюдения только усугубляется тем фактом, что алгоритмы распознавания лиц регулярно приводят к ошибочной идентификации, включая обнаружение того факта, что такие алгоритмы с гораздо большей вероятностью неверно идентифицируют расовых людей и женщин по сравнению белыми мужчинами.

Рекомендация 2: Правоохранительным органам следует улучшить целостность полицейских баз данных и методы управления, в том числе расширить возможности отдельных лиц проверять и исправлять точность личной информации, хранящейся в полицейских базах данных.

Существующие полицейские базы данных часто изобилуют предвзятыми и неточными данными, и любая технология алгоритмического полицейского контроля, которая полагается на такие базы данных, рискует воспроизвести и усилить такие предубеждения и неточности. Правоохранительные органы и

система правосудия должны разработать процессы для успешного обслуживания и обновления таких баз данных (например, баз данных о судимости, баз данных, содержащих данные о задержании полиции), особенно когда данные, содержащиеся в них, будут обрабатываться алгоритмической полицейской технологией.[1393] Правоохранительные органы в большинстве провинций уже подчиняются значимым стандартам точности данных в соответствии с законодательством о конфиденциальности в Канаде. Тем не менее, стандарты точности данных должны быть усилены сетью значимых сдержек и противовесов, включая регулярные аудиты и рекомендации технических экспертов в сочетании с экспертами в области прав на неприкосновенность частной жизни и уголовного правосудия в отношении применимых передовых методов управления базами данных в отношении алгоритмических технологий.

Только данные, которые подлежат стандартам точности данных, подкреплённые адекватными системами сдержек и противовесов, должны рассматриваться для алгоритмической обработки в целях уголовного правосудия при соблюдении всех других критериев (например, тех, которые изложены в этих рекомендациях или установлены в результате судебного расследования).

Рекомендация 3: Правительствам следует прямо регулировать хранение и уничтожение биометрических данных правоохранительными органами.

Сбор и хранение личной информации, такой как отпечатки пальцев и фотографии из кружки, защищены разделом 8 Хартии и законодательством о конфиденциальности. Тем не менее, отдельные полицейские службы придерживаются различных политик в отношении уничтожения биометрических данных (например, отпечатков пальцев, фотографий с кружка), и, в большинстве случаев, уничтожение является системой на основе запросов (т.е. отдельные лица должны требовать уничтожения своих данных, в отличие от данных, которые регулярно уничтожаются в соответствии с внутренней политикой). Текущие процессы, посредством которых человек может потребовать уничтожения записей после рассмотрения его дела, также непоследовательны, расплывчаты или чрезмерно дискреционны. Чёткое государственное регулирование необходимо для стандартизации политики полиции, усиления защиты конфиденциальности и предоставления рекомендаций по приведению практики в соответствие с принципами

[1393] Brigitte Bureau, «RCMP database remains out of date, police and prosecutors say", CBC News (10 March 2015) <https://www.cbc.ca/news/politics/rcmp-database-remains-out-of-date-police-and-prosecutors-say-1.2989397>.

необходимости и соразмерности. Запрос на уничтожение данных или записей должен быть бесплатным для физических лиц. Данные должны автоматически и незамедлительно уничтожаться в случаях, когда обвинения не предъявляются или, когда обвинения остановлены, отклонены или сняты.

Рекомендация 4: Федеральному правительству следует реформировать положения Уголовного кодекса о судебных ордерах, чтобы конкретно рассмотреть вопрос об использовании алгоритмической полицейской технологии правоохранительными органами.

Один из наиболее важных способов защиты интересов частной жизни - обеспечить, чтобы действия правоохранительных органов, вторгающиеся в жизнь людей, находились под осмысленным надзором. Отсутствие надзора обычно делает методы правоприменения, затрагивающие интересы конфиденциальности, неконституционными.[1394] Традиционно такой надзор означал получение предварительного разрешения от судей (например, в форме ордера или производственного приказа) до того, как правоохранительные органы предпримут действия, нарушающие конфиденциальность любого человека. Следуя этой модели, необходимо получить судебные ордера, прежде чем правоохранительные органы смогут проводить алгоритмическую обработку данных по ранее собранным данным. В то время как общие ордера обеспечивают всеобъемлющую процедуру для полицейских методов, которые иначе не регулируются другими механизмами ордеров или производственных приказов, Парламенту следует реформировать Уголовный кодекс, чтобы конкретно рассмотреть вопрос об использовании правоохранительными органами алгоритмических полицейских технологий. Такая реформа должна конкретно касаться методов обработки данных, которые включают в себя поиск или изъятие данных правоохранительными органами с целью алгоритмического анализа того типа, который рассматривается в этом отчёте, включая «прогнозную» аналитику. Например, в то время как существующий режим надзора в Уголовном кодексе регулирует судебно-медицинский анализ ДНК, он не даёт каких-либо конкретных указаний или чётких ограничений на использование биометрических данных и программного обеспечения для распознавания лиц на фотографиях, которые уже находятся в распоряжении полиции (которые были собраны для других целей). Для устранения этого дефицита необходимо провести правовую реформу.

[1394] See e.g., R v Tse, 2012 SCC 16.

Рекомендация 5: Федеральные и провинциальные законодательные органы должны пересмотреть и модернизировать законодательство о конфиденциальности с особым вниманием к переоценке текущих мер защиты с учётом передовых возможностей технологий алгоритмического контроля.

Все полицейские службы Канады подчиняются федеральному или провинциальному законодательству о конфиденциальности. Законодательство о конфиденциальности играет важную роль в регулировании минимальных стандартов, которым должны соответствовать правоохранительные органы при сборе, обработке или раскрытии личной информации человека. Парламент и законодательные собрания должны пересмотреть законодательство о конфиденциальности и, при необходимости, обновить его, чтобы наилучшим образом регулировать использование больших данных правоохранительными органами с помощью алгоритмических технологий. Например, законодательство о конфиденциальности часто устанавливает исключения и разрешения для деятельности, связанной с правоохранительными органами. Хотя такие исключения по большей части включались и разрабатывались в то время, когда рассматривались более традиционные действия полиции, те же исключения, к сожалению, теперь можно было изменить, чтобы освободить современные алгоритмические полицейские технологии от столь необходимых мер контроля конфиденциальности. Таким образом, эти исключения должны быть реформированы, чтобы в достаточной мере защитить стандарты соразмерности и необходимости. В частности, потенциальные области для обзора и реформы должны включать в себя способ, которым законодательство о конфиденциальности регулирует сбор, обработку и раскрытие метаданных, биометрических данных, личных данных в общественных местах, механизмы обмена информацией, механизмы возмещения ущерба и последствия невыполнения защиты личной информации.[1395]

Рекомендация 6: Правоохранительные органы должны проявлять крайнюю осторожность, чтобы избежать неконституционной практики обмена данными с частным сектором и государственными органами, не относящимися к полиции.

[1395] See for example, Report of the Standing Committee on Access to Information, Privacy and Ethics, «Protecting the Privacy of Canadians: Reform of the Privacy Act», (December 2016), <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP8587799/ethirp04/ ethdirp04-e.pdf>.

К регламентированной практике обмена данными между правоохранительными органами и другими государственными структурами, такими как агентства социальных услуг, школы или органы общественного транспорта, или частным сектором, следует обращаться с особой осторожностью. Такая осторожность, включая полное недопущение, где это возможно, требуется, поскольку механизмы обмена данными, при которых данные передаются от органов, не связанных с правоохранительными органами, к правоохранительным органам, могут привести к конституционным обязательствам для первых, которые неизбежны по закону, но не работают на практике, что приводит к неприемлемой ситуации в отношении соблюдения права на неприкосновенность частной жизни, указанного в разделе 8.

В частности, если государственная или частная организация участвует в формальном или постоянном обмене данными с целью оказания помощи полиции в правоохранительной деятельности, эта организация может непреднамеренно стать связанной конституционными обязательствами в отношении конфиденциальности согласно разделу 8 или доктрине правоохранительных органов. Такие обязательства могут включать требование о получении судебного ордера при сборе частных данных до их передачи в полицию. Однако юридические лица, не связанные с правоохранительными органами, не только не привыкли соблюдать конституционные гарантии, обычно применяемые полицией к использованию частной информации, но и с точки зрения закона и практики они не смогут заставить себя поступать в соответствии с Конституцией, даже если они попытаются, потому что судебные ордера доступны только правоохранительным органам.

Таким образом, договоренности об обмене данными между правоохранительными органами и другими правительственными учреждениями или организациями частного сектора для целей охраны правопорядка, вероятно, не могут существовать в соответствии с Конституцией, не вызывая серьёзных и сложных разветвлений для практики сбора данных такими неполицейскими организациями.

Для защиты от неконституционных механизмов обмена данными любые случаи обмена данными с правоохранительными органами, государственными субъектами, не являющимися полицейскими, или организациями частного сектора, должны быть официально задокументированы в меморандумах о взаимопонимании, и такие меморандумы должны быть представлены соответствующим уполномоченным по конфиденциальности для ознакомления и для целей публичной записи. Как правило, данные от агентств государственного и частного секторов не должны передаваться в распоряжение правоохранительных органов. Эти субъекты, не относящиеся к полиции, должны соблюдать свои собственные обязательства в отношении

конфиденциальности, которые регулируют законное обращение и защиту личных данных и прав отдельных лиц.

6.2. Рекомендация по защите прав на свободу выражения мнений, мирных собраний и ассоциаций

Технологии алгоритмической полицейской деятельности и, в частности, методы алгоритмического наблюдения, могут препятствовать осуществлению прав на свободу выражения мнений, мирных собраний и ассоциаций. Технологии алгоритмической полицейской деятельности подчёркивают особенно тесную связь между правом на неприкосновенность частной жизни и этими основными свободами, каждая из которых защищена международным правом прав человека и разделом 2 Хартии. Например, инструменты алгоритмического наблюдения, такие как технология распознавания лиц и программное обеспечение для наблюдения в социальных сетях, угрожают анонимности толпы, которая традиционно защищала личности протестующих на открытом воздухе и в сети.[1396] а также может оказывать сдерживающее воздействие на защищаемые свободы[1397]; об этих пугающих эффектах свидетельствовали официальные исследовательские интервью, проведённые для этого отчёта, и они были установлены в ходе научных исследований. Такое охлаждение происходит отчасти из-за исторического и текущего контекста непропорционального надзора со стороны правоохранительных органов против расового правосудия и защитников прав коренных народов. Рекомендация в этом разделе сосредоточена на обеспечении того, чтобы использование алгоритмической полицейской технологии было необходимым и соразмерным законным целям, относительно потенциального значительного ущерба правам на свободу выражения мнений, мирных собраний и ассоциаций в результате использования такой технологии.

Рекомендация 7. Правоохранительные органы должны получить предварительное судебное разрешение на развёртывание технологии алгоритмического наблюдения на публичных собраниях и в онлайн-среде.

Если используются алгоритмические методы наблюдения, использование таких методов должно быть предметом предварительного судебного разрешения в свете повышенных интересов конфиденциальности,

[1396] See Section 5.2.1 («Data Collection: Mass Surveillance and Public Space").
[1397] See Section 5.3 («Rights to Freedom of Expression, Peaceful Assembly, and Association").

поставленных на карту, и конституционной защиты согласно разделу 2, касающемуся соразмерности и необходимости. Ордер должен быть основан на разумных и вероятных основаниях того, что существует конкретная угроза и что использование метода даст результаты, необходимые для устранения этой угрозы.

Правительственные органы не могут юридически оправдать мониторинг выразительной или ассоциативной деятельности на основе мониторинга политической активности как таковой. Например, согласно Закону о безопасности Канады о раскрытии информации, «пропаганда, протест, несогласие или художественное выражение не являются деятельностью, которая подрывает безопасность Канады».[1398] Ограничения права на мирные собрания должны быть нейтральными по содержанию и не основываться на расе, этнической принадлежности, политических взглядах, сексуальной ориентации или других защищаемых или смежных факторах, при этом сохраняя внимание к потенциальной косвенной дискриминации через неблагоприятные воздействия.[1399]

6.3. Рекомендации по защите права на равенство и свободу от дискриминации

Алгоритмические методы работы полиции могут нарушать права определённых лиц на равенство и свободу от дискриминации посредством дискриминации неблагоприятного воздействия. Кажущееся «нейтральным» применение инструментов алгоритмической полицейской деятельности маскирует реальность того, что они могут непропорционально сильно влиять на маргинализированные сообщества в категории, защищённой законом о равенстве (те. сообщества, основанные на таких характеристиках, как раса, этническая принадлежность, сексуальная ориентация или инвалидность). Исторический и продолжающийся чрезмерный надзор, более суровое обращение и систематическая предвзятость в системе уголовного правосудия - все это приводит к тому, что данные полиции отражают исторические неблагоприятные условия и дискриминацию, налагаемую на определённые группы, такие как чернокожие и коренные народы, сообщество ЛГБТК, людей, страдающих психическим воздействием болезни, люди, не имеющие жилья или иным образом находящиеся в социально-экономическом положении, а также другие уязвимые группы населения. Данные полиции также свидетельствуют о

[1398] Security of Canada Information Disclosure Act, SC 2015, c 20, s 2.

[1399] Верховный суд Канады четко указал, что Хартия должна толковаться как единая система, которая сохраняет свои основополагающие ценности и является внутренне согласованной на протяжении всего периода. Подсектор медицинских услуг и вспомогательных учреждений. Health Services and Support-Facilities Subsector Bargaining Assn v British Columbia, [2007] 2 SCR 391 at paras 80-86; R v S (RJ), [1995] 1 SCR 451 at 561.

недостаточном контроле над теми же сообществами, когда они становятся жертвами, или о преимущественном нежелании правонарушителей из доминирующих социальных классов. Многочисленные неточности, предвзятости и другие источники недостоверности присутствуют в большинстве распространённых источников полицейских данных в Канаде. В результате сделать надёжные выводы на основе исторических данных полиции, вероятно, невозможно, и, следовательно, любое использование технологии алгоритмической полицейской деятельности, основанной на таких данных, вероятно, является неконституционным согласно разделу 15 Хартии.

Некоторые канадские правоохранительные органы, которые используют или рассматривают возможность использования алгоритмических полицейских технологий, включили определённые меры для предотвращения или смягчения потенциальной дискриминационной предвзятости, связанной с такими технологиями. Например, Департамент полиции Ванкувера удаляет инциденты, о которых сообщает полиция, из данных, используемых для обучения их технологии алгоритмического контроля местоположения (система алгоритмического прогнозирования GeoDASH). Однако сомнительно, что предвзятость в системе уголовного правосудия может быть существенно уменьшена, если алгоритмы полагаются на наборы данных, отражающие историческую и текущую систематическую предвзятость (которая также обычно отражается в отчётах об инцидентах, инициированных представителями общественности). Следует проявлять крайнюю осторожность, прежде чем правоохранительным органам будет разрешено, если вообще будет разрешено, использовать алгоритмические полицейские технологии, потому что эти инструменты могут усугубить и без того неконституционное и разрушительное воздействие, которое может вызвать системное нацеливание на маргинализированные сообщества (например, за счёт повышенной видимости данных в результате доступа службы социального обеспечения). Кроме того, методы, которые могли бы независимо оценивать или проверять точность и надёжность технологий алгоритмического контроля, либо отсутствуют, либо еще не разработаны. Следующие три рекомендации сделаны в свете глубокой неуверенности в том, можно ли использовать алгоритмические технологии полицейского контроля таким образом, чтобы не допускать дискриминации или иным образом несправедливо воздействовать на лиц, защищённых разделом 15.

Рекомендация 8: Федеральному правительству следует провести судебное расследование для проведения всесторонней проверки возможности использования правоохранительными органами исторических наборов полицейских данных для использования в технологиях алгоритмической полицейской деятельности.

Федеральное правительство должно провести национальное судебное расследование, чтобы изучить возможность использования алгоритмической полицейской технологии, которая обрабатывает массивы полицейских данных. Изучение использования исторических наборов полицейских данных с целью предотвращения дискриминации неблагоприятных воздействий в Канаде имеет решающее значение в свете обязательств правительства в соответствии с Хартией, международным правом прав человека и текущими процессами примирения с общинами коренных народов в Канаде. Объём расследования должен включать полномочия на изучение объёма наборов полицейских данных, доступных правоохранительным органам, для изучения системных предубеждений, которые могут присутствовать в таких наборах данных, и для тщательного изучения правоохранительной практики, связанной с хранением данных. Судебное расследование должно, в частности, быть сосредоточено на разработке руководства, разъясняющего меры защиты, предусмотренные разделом 15, для оказания помощи правоохранительным органам, государственным деятелям и участникам системы правосудия, которые могут участвовать в судебных процессах и оценке алгоритмических технологий в соответствии с разделом 15. Эта рекомендация сделана частично из-за относительно недостаточно развитой юриспруденции в соответствии с разделом 15 Хартии в отношении правительственной деятельности (т.е. действий, предпринятых правоохранительными органами на основе выводов или прогнозов алгоритмической полицейской технологии), в отличие от государственного законодательства. Правоохранительным органам, юрисконсультам и лицам, участвующим в системе уголовного правосудия, была бы полезна помощь в разъяснении обязанностей государства.

Рекомендация 9: Правительства должны ввести мораторий на использование правоохранительными органами технологий, основанных на алгоритмической обработке исторических массивов полицейских данных, до проведения всестороннего анализа.

Хартия запрещает государственную деятельность, которая увековечивает или причиняет какие-либо предрассудки или ущемление интересов отдельных лиц на основе различий, проводимых на защищённых основаниях в соответствии с разделом 15.

Все уровни правительства (т.е. муниципалитетов, провинциальных правительств и федерального правительства), наделённых законодательными полномочиями в отношении правоохранительных органов, должны установить

мораторий на технологии, основанные на алгоритмической обработке исторических наборов полицейских данных. Установление таких мораториев предотвратило бы дальнейшее нанесение вреда или материализацию выявленных рисков для прав человека, одновременно предоставляя время для завершения необходимой, всеобъемлющей и целостной оценки (как рекомендовано в Рекомендации 8) того, возможно ли использовать алгоритмические полицейские технологии способом, который не нарушает неконституционные права лиц, защищаемых статьей 15, путём увековечения дискриминации, предотвращению которой служит статья 15.

Рекомендация 10: Правоохранительные органы должны внедрить постоянное наблюдение для отслеживания потенциальных проявлений предвзятости при использовании любой технологии алгоритмического контроля.

Любое использование алгоритмических полицейских технологий должно сопровождаться практиками мониторинга, которые внимательно следят за шаблонами, отражающими предвзятость, например, предвзятость по отношению к маргинализованным или исторически угнетённым сообществам. Мониторинг должен, насколько это возможно, сопоставлять результаты алгоритмических оценок с внешними источниками и дисциплинами (например, доказательствами социальных наук, отчётами о правах человека, консультациями или жалобами сообщества), чтобы установить, присутствует ли чрезмерная предвзятость в алгоритмических инструментах. В некоторых случаях предвзятость по отношению к защищенным группам может быть обнаружена при просмотре доверенных данных, которые имеют тенденцию коррелировать с исторической дискриминацией, с которой сталкивались защищённые группы. Прокси-серверы могут включать в себя кажущиеся безобидными индикаторы (например, интересы в социальных сетях, историю покупок), которые на практике связаны с потенциально конфиденциальными данными, такими как социально-экономический статус, раса или этническая принадлежность, географическое положение, зависимость от государственных услуг или индикаторы, связанные с лечение психического здоровья.

6.4. Рекомендация по защите права на свободу и свободу от произвольного задержания

Хартия и международное право прав человека гарантируют право на свободу, включая право не подвергаться задержанию или произвольному аресту (согласно разделам 7 и 9 Хартии соответственно). Основываясь на конституционных и международных обязательствах в области прав человека, правоохранительные органы должны иметь разумные основания (т.е. достаточно веские и объективные) для вмешательства в свободу человека путём задержания или ареста человека. Это закрепленное в конституции требование разумных оснований не позволяет правоохранительным органам полагаться на обобщённые прогнозы, сделанные с помощью алгоритмических полицейских технологий, в качестве основы для задержания или ареста человека. По своей конструкции алгоритмические полицейские технологии обычно основываются на обобщённых или стереотипных выводах о риске. Это запрещённые основания для оправдания посягательства на свободу человека.[1400]

Обобщённый характер алгоритмических предсказаний – не единственная проблема, которая не позволяет технологиям алгоритмического контроля стать подходящими инструментами для оправдания вмешательства в свободу. Правоохранительные органы также не могут оправдать арест или задержание недостоверной информацией. Технологии алгоритмической полицейской деятельности остаются непроверенными, и во многих случаях алгоритмы обучаются с использованием предвзятых полицейских данных.

Рекомендация 11: Правоохранительным органам следует установить полный запрет на использование алгоритмических прогнозов для оправдания вмешательства в личную свободу.

Правоохранительные органы и связанные с ними надзорные органы должны гарантировать, что алгоритмические полицейские технологии не используются для ограничения свободы личности путём задержания и ареста. Для реализации конституционного императива, согласно которому нельзя полагаться на алгоритмические прогнозы для оправдания вмешательства в свободу, в этом отчёте рекомендуется, чтобы правоохранительные органы устанавливали и применяли письменные правила, которые конкретно запрещают использование технологий алгоритмического контроля в качестве основания для задержания или ареста. Чёткий запрет на использование

[1400] Этот вывод не обязательно применим ко всем алгоритмическим технологиям управления. Некоторые формы алгоритмических технологий наблюдения могут быть достаточно надежными и специфичными для конкретного случая, так что доказательства, полученные в результате использования технологии, могут рассматриваться сотрудником полиции при формировании оснований для проведения задержания или ареста. Например, автоматический считыватель номерных знаков может фиксировать четкое изображение номерного знака, который соединен с приостановленной лицензией, что будет представлять собой более надежное доказательство, чем алгоритмический вывод или обобщение.

алгоритмических прогнозов для оправдания действий полиции, таких как остановки, задержания и аресты, необходим из-за неадекватности альтернативных мер защиты, которые можно было бы рассмотреть. Опасности, связанные с необоснованными и предвзятыми действиями полиции, слишком велики.

Такие риски неконституционных нарушений права на свободу возникают из-за, в частности, двух форм предвзятости: бессознательной предвзятости, основанной на защищаемых характеристиках, которая приводит к таким проблемам, как расовое профилирование, и предвзятости автоматизации, которая представляет собой тенденцию людей полагаться на технологии в качестве превосходит человеческое суждение, даже если у них есть основания полагать, что технология несовершенна или некорректна.

Хотя исследования из других областей показали, что некоторые формы обучения или методы смягчения последствий могут снизить систематическую ошибку автоматизации в некоторых случаях, результаты в целом были неоднозначными.[1401]

Следует подчеркнуть, что такие меры, даже если они безупречно реализованы и соблюдаются на практике, не могут искоренить предвзятость автоматизации.[1402] Таким образом, такого обучения и мер по смягчению последствий недостаточно, чтобы гарантировать, что использование алгоритмических полицейских технологий при принятии полицейских решений не приведёт к нарушениям прав человека через необоснованные ограничения свободы личности. Это конкретное использование алгоритмического контроля должно быть полностью запрещено технологически.

[1401] Смотрите, например, "Агентства должны дать понять слушателям из числа офицеров, что автоматизированные системы ошибочны. С этой целью слушатели должны пройти четкую подготовку по проблеме предвзятости в области автоматизации. Исследования показывают, что лица, которые проходят такую подготовку, чаще изучают предложения автоматизированной системы. Подготовка судей была эффективной на параллельном предприятии. Специальные семинары по научной теории и методологии обеспечили необходимую подготовку судей федеральных окружных судов, отвечающих за оценку достоверности показаний экспертов. [...] [A] гении должны требовать, чтобы должностные лица, проводящие слушания, подробно объясняли, что они полагаются на решение автоматизированной системы. Сотрудники должны определять компьютеризированные факты или юридические выводы, на которые они опираются при принятии своих решений. Это согласуется с давней верой административного права в профилактическую силу требования четкого изложения причин. Обращение к слушателям с просьбой оценить основу своих решений позволит еще больше смягчить последствия предвзятости автоматизации ". Danielle Keats Citron, «Technological Due Process» (2008) 85:6 Washington University Law Review 1249 at 1306-07 (footnotes omitted); Osonde Osoba & William Welser IV, «An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence», RAND Corporation (2017) at 23-24 <https://pdfs.semanticscholar.org/b7be/0be36706c30a76312b34d60ff02d97698191. pdf>; and Kate Goddard, Abdul Roudsari & Jeremy C Wyatt, «Automation bias: a systematic review of frequency, effect mediators, and mitigators" (2012) 19 Journal of the American Medical Informatics Association 121 at 125.

[1402] See e.g., John Zerilli, Alistair Knott, James Maclaurin & Colin Gavaghan, «Algorithmic Decision-Making and the Control Problem» (2019) 29 Minds and Machines 555 at 575.

6.5. Рекомендации по защите прав на надлежащую правовую процедуру и средства правовой защиты (подотчётность и прозрачность)

Надёжные процессуальные гарантии защищают основные права человека, нарушенные правоохранительной деятельностью. Центральным способом защиты прав человека и международных прав человека, включая право на надлежащую правовую процедуру и право на средство правовой защиты от нарушений прав, является разработка надёжных механизмов подотчётности посредством всеобъемлющей системы сдержек и противовесов.

Механизмы подотчётности позволяют парламентариям, прессе, судам, организациям гражданского общества, адвокатам по уголовным делам и широкой публике иметь доступ к информации и справедливым процессам, с помощью которых они защищаются от нарушений прав и устанавливают измеримые стандарты для проверки поведения правоохранительных органов.

Правовой ландшафт надзорных органов полиции представляет собой сложную мозаику из образований. К таким структурам относятся гражданские органы надзора за полицейскими службами, государственные уполномоченные по вопросам конфиденциальности и прав человека, суды, общественные расследования и системные проверки, а также советы полицейских служб. Режимы полицейского надзора включают и уравновешивают основополагающий принцип правовой системы Канады, который уважает независимость полиции от определённых форм политического вмешательства.[1403]

Если в Канаде правоохранительные органы будут продолжать использовать алгоритмические полицейские технологии, все эти элементы надзора будут играть свою роль. В результате следующие девять рекомендаций сосредоточены на механизмах координации надзора за счёт развития институционального опыта, руководства и подотчётности в этом сложном ландшафте.

Рекомендация 12: правоохранительные органы должны быть незамедлительно и полностью прозрачными для общественности и уполномоченных по конфиденциальности в отношении всех видов использования технологий алгоритмического контроля.

[1403] See Kent Roach, «Models of Civilian Police Review: The Objectives and Mechanisms of Legal and Political Regulation of the Police" (2014) 61 Criminal Law Quarterly 29; Kent Roach, «Police Government Relations and Police Independence" (June 2017), <https://www.cepcsj.gouv.qc.ca/fileadmin/documents_client/recherche/Quebec_Police_Independence_pour_depot.pdf> .

Правоохранительные органы по всей Канаде должны немедленно и публично раскрывать информацию о любых алгоритмических технологиях полицейского контроля, которые рассматриваются, разрабатываются, закупаются, тестируются или используются для целей полицейской деятельности. Агентства должны оперативно делать общедоступными информацию о любом текущем использовании или тестировании технологии алгоритмической полицейской деятельности в качестве промежуточного шага до тех пор, пока не будут установлены другие долгосрочные и постоянные меры прозрачности и подотчётности (как будет подробно описано в Рекомендациях 13 и 14).

Правоохранительные органы Канады также должны срочно начинать или расширять раскрытие информации и диалог с уполномоченными по вопросам информации и конфиденциальности на федеральном и региональном уровнях в отношении всех технологий алгоритмического контроля, которые рассматриваются, закупаются, тестируются или развёртываются в целях охраны. Принятие надёжного набора практик прозрачности имеет решающее значение в свете того, насколько продуктивными обсуждениями часто являются понимание всеми сторонами обсуждаемых технологий. Упреждающее раскрытие информации должно широко применяться в качестве передовой практики среди всех правоохранительных органов в будущем.

Рекомендация 13: Правительства и правоохранительные органы должны привлекать внешних экспертов, в том числе экспертов из исторически маргинализированных сообществ, на которые непропорционально сильно влияет система уголовного правосудия, для разработки механизмов регулирования и надзора за технологиями алгоритмического контроля в рамках выполнения алгоритмической оценки воздействия любых таких технологий, которые были введены в действие.

Исторически маргинализованные сообщества, которые подвергаются системной дискриминации в системе уголовного правосудия, должны быть вовлечены в любые процессы по разработке, внедрению или мониторингу алгоритмических полицейских технологий, включая соответствующие механизмы регулирования и надзора. Эти сообщества могут указывать причины или разъяснять, почему данная технология является несоответствующей, незаконной, ненужной, вредной или неоправданно навязчивой, о чём правоохранительные органы или правительства могут не знать. Затронутые сообщества могут также предложить альтернативные или

более эффективные меры для решения конкретной проблемы вместо предлагаемой технологии или определить более насущную проблему, требующую внимания. Кроме того, к любым консультациям следует привлекать независимых экспертов, таких как юристы, специалисты по расовому правосудию, а также исследователи технологий и прав человека, технологи, представляющие общественные интересы, или исследователи в области безопасности, чтобы правовые, политические и технические аспекты предлагаемой технологии алгоритмической полицейской деятельности были адекватно оценены в процессе консультаций. Любые консультации с представителями сообщества или другими экспертами должны включать справедливую компенсацию за их время и опыт. Один из возможных подходов состоит в том, чтобы следовать моделям, принятым Канадской комиссией по радио, телевидению и электросвязи и другими административными судами, которые предоставляют финансирование для обеспечения участия в судебных разбирательствах, представляющих общественный интерес.

Рекомендация 14: Правительствам провинций следует принять директивы по использованию и закупке технологий алгоритмической полицейской деятельности.

Правительства провинций должны принять министерские директивы, требующие, чтобы все виды использования алгоритмических полицейских технологий – в той мере, в какой они не запрещены мораторием или конституционным запретом – полностью соответствовали общегосударственной директиве, регулирующей ответственное развитие и использование этих технологий.[1404] Отчёт Иппервошского расследования в Онтарио поддерживает использование министерских директив в качестве метода введения регулирующего надзора за правоохранительной деятельностью в области, вызывающие особую озабоченность с точки зрения прав человека.[1405]

[1404] Пример такой директивы см. в: <https://seattle.legistar.com/LegislationDetail.aspx?ID=2981172&GUID=0B2FEFC0-822F-4907-9409-E318537E5330&FullText=1>, где городской совет Сиэтла издал закон, регулирующий приобретение и использование оборудования для наблюдения, вызванный обеспокоенностью по поводу конфиденциальности и отсутствия процесса приобретения городом технологий наблюдения, таких как беспилотники и установка видеокамер вдоль набережной Сиэтла и в центре города.

[1405] В докладе рекомендуется издать ряд министерских директив для правоохранительных органов Онтарио в целях реагирования на конкретные вопросы прав человека и полицейской деятельности, которые были предметом этого расследования: Сидни Б. Линден, Доклад о расследовании по делу Ипперваш (Торонто: опубликовано Министерством Генерального прокурора, Королевский принтер Онтарио, 2007 год). Как указано в документе IN FOCUS # 2: Overview of the Canadian Criminal Justice System (Обзор канадской системы уголовного правосудия), полицейские службы в Канаде подпадают под юрисдикцию провинций, и поэтому правительства провинций имеют право осуществлять надзор на основе официальных директив.

Директивы провинций относительно ответственного развития и использования технологий алгоритмического контроля должны включать следующие ключевые требования:

- Требование о том, чтобы правоохранительные органы завершили алгоритмическую оценку воздействия перед использованием алгоритмической системы полицейского контроля в соответствии со стандартизированной структурой, которая явно оценивает соблюдение международного права прав человека и Хартии. Эта оценка воздействия должна включать оценку надёжности, необходимости и соразмерности с сопутствующим запретом на использование алгоритмических технологий, которые, как предполагается, потенциально могут привести к непропорциональному воздействию на права человека.[1406]
- Для алгоритмических полицейских технологий, которые могут нарушить Хартию и права человека, необходимо предварительное одобрение министерства наряду с предварительными консультациями с уполномоченными по конфиденциальности.
- Строгие требования к независимой проверке и научному подтверждению (опубликованы для обеспечения публичной отчётности и проверки в судебных разбирательствах) алгоритмов, лежащих в основе полицейских технологий, до их использования; они должны оценивать точность, справедливость и статистическую или дискриминационную предвзятость. Для облегчения независимой проверки потребуются контракты на независимость с компенсацией.
- Требование к правоохранительным органам, использующим технологию алгоритмического контроля, должна проактивно публиковать информацию, например, через портал открытых данных, о типах данных обучения и оперативных данных полиции, используемых в алгоритмах. Отчёты должны включать демографическую информацию, включая, в частности, данные с разбивкой по расовому признаку. Одну модель такого подхода можно найти на портале данных Чикаго, на котором опубликованы данные, использованные для создания прекращенного сейчас алгоритма оценки рисков Департаментом полиции Чикаго, известного как список стратегических субъектов (SSL).[1407] Портал открытых данных должен обеспечивать прозрачность того, как технологии

Муниципалитеты могут также регулировать деятельность муниципальных правоохранительных органов в тех случаях, когда делегирована провинциальная ответственность, а федеральные и провинциальные органы могут регулировать деятельность RCMP.

[1406] Для получения дополнительной информации см. раздел "IN FOCUS # 8: Algorithmic Impact Assessments" в разделе 5.6.3. Заключительные замечания: Технология алгоритмической политики и должная процедура.or more details, see «IN FOCUS #8: Algorithmic Impact Assessments", in Section 5.6.3. Concluding Comments: Algorithmic Policing Technology and Due Process.

[1407] «Strategic Subject List" (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>.

алгоритмического контроля используют, обрабатывают и полагаются на данные; должны предоставлять данные в формате, доступном для независимого использования и перекрёстных ссылок с другими наборами данных; и должен быть ясным в отношении данных которые не предоставляются, потому что они не существует, или потому, что они не были собраны.[1408] Любые открытые данные и аналогичные инициативы по раскрытию информации должны осуществляться с должной осторожностью в отношении потенциального ущерба и нарушений конфиденциальности в зависимости от типа предоставленных данных.[1409] Как предупредила Тереза Скасса, законы о конфиденциальности в государственном секторе, которые применяются к правоохранительным органам, «требуют от государственных органов защиты частной жизни путём уравновешивания прав на неприкосновенность частной жизни и общественного интереса в раскрытии личной информации. В случаях, когда личная информация носит очень конфиденциальный характер, права на неприкосновенность частной жизни обычно имеют приоритет над раскрытием информации».[1410]

- Требование, чтобы все принятые алгоритмические полицейские технологии были совместимы с надёжной структурой процессуальной справедливости и надлежащей правовой процедуры при реализации алгоритмических методов, включая, требования о том, что правоохранительные органы имеют возможность предоставить полное раскрытие информации в уголовном процессе.[1411]
- Никакое решение или действие субъекта системы правосудия (должностное лицо правоохранительных органов или в уголовном суде), которые затрагивают конституционные интересы или интересы человека, защищаемые правами человека, не принимаются только в результате алгоритмической системы (т.е. всегда должен присутствовать человек в петле).

[1408] Смотрите, например, "[F] или пример, если нажать на" сексуальные преступления "в городе, который не предоставляет эти данные, то полученная карта не покажет никаких сексуальных преступлений в обыскиваемой области, что может предложить пользователю, что такие преступления не имели места в течение указанного периода времени, а не что данные отсутствуют". Teresa Scassa, «Police Service Crime Mapping as Civic Technology: A Critical Assessment» (2016) 5:3 International Journal of E-Planning Research 13 at 20

[1409] См., например, (в контексте картирования преступлений, но применимого в тех случаях, когда аналогичные детали предаются гласности, даже если они не визуализируются на карте): "Соображения конфиденциальности могут также влиять на картирование других данных о преступлениях. Например, некоторые полицейские силы предпочитают не выявлять преступления, связанные с насилием в семье или сексуальными надругательствами над детьми, по соображениям неприкосновенности частной жизни. Такие преступления часто происходят внутри дома, и картирование даже до уровня 100 блоков может привести к идентификации либо жертвы, либо исполнителя (или к вредным неправильным предположениям об их личности) ".

[1410] Ibid.

[1411] Для получения более подробной информации об объеме обязательств по обязательному раскрытию информации в отношении алгоритмической технологии контроля см. раздел 5.6.2 ("Неразглашение информации и право на полный ответ и защиту").

- Любое использование технологии алгоритмического контроля должно включать статистическое отслеживание и формальный процесс документирования всех известных ошибок и инцидентов (например, утечки данных, взлома).
- Использование алгоритмических полицейских технологий должно происходить таким образом, чтобы не допускать ошибки в отношении осторожности, чтобы избежать нарушений прав лиц или групп, находящихся в неблагоприятном маргинальном положении.
- Правовые стандарты общественных интересов и контроль со стороны государственного сектора должны применяться к коммерческим поставщикам, которые заключают контракты с правительством или правоохранительными органами на инструменты алгоритмического контроля, когда на карту поставлена уголовная опасность. Такие инициативы могут следовать модели лаборатории прогнозной аналитики полиции Саскачевана, которая в соответствии с протоколом разрабатывает свои технологии прогнозной аналитики самостоятельно и в сотрудничестве с академическими экспертами.
- Правоохранительные органы должны сообщать ясным языком на общедоступных веб-сайтах всякий раз, когда решение будет принято на основе алгоритмической системы принятия решений. Кроме того, лица, на которых повлияло решение правительства, которое было принято полностью или частично с помощью автоматизированной системы принятия решений, должны получить содержательное объяснение того, как и почему было принято решение.

Рекомендация 15: Федеральному правительству следует расширить положения Уголовного кодекса о парламентской отчётности, которые в настоящее время применяются только к определённым методам электронного наблюдения.

Федеральному правительству следует рассмотреть возможность расширения требований к парламентской отчётности, которые изложены в Уголовном кодексе и которые в настоящее время применяются к живому электронному слежению за частными сообщениями. В соответствии с существующей структурой федеральное и провинциальные правительства должны представлять Парламенту годовые отчёты с информацией относительно разрешений на перехват частных сообщений. Годовые отчеты готовятся в сотрудничестве с RCMP и провинциальными и муниципальными службами полиции. Теоретически их обновление могло бы помочь общественности понять использование новых технологий.

Парламенту также следует рассмотреть возможность расширения механизмов публичной отчётности, чтобы эти механизмы обеспечивали лучший контекст использования технологии алгоритмической полицейской деятельности. В частности, Парламент может потребовать от правительств включать в представленный годовой отчёт описание конкретных видов технологий, которые были приняты или находятся на рассмотрении. В этом повествовании можно также обсудить, зачем нужны такие технологии. Аналогичные требования могут быть установлены путём парламентской реформы для аналогичных отчётов, которые ежегодно представляются генеральными солиситорами провинции. Преимущество расширения типа информации, подлежащей публичной отчётности, заключается в том, что такая расширенная отчётность позволит законодательным органам и общественности требовать от правительств и правоохранительных органов учёта технологий алгоритмического контроля за их воздействием и использованием ими публичных данных при использовании финансирования.

Рекомендация 16: Уполномоченные по вопросам конфиденциальности и прав человека должны быть наделены полномочиями и обеспечены достаточным финансированием и ресурсами для инициирования и проведения расследований использования правоохранительными органами технологии алгоритмического контроля.

Технологии алгоритмического контроля требуют целенаправленного надзора со стороны уполномоченных по вопросам конфиденциальности, которые особенно хорошо подходят для оценки того, как новые технологии могут неправомерно посягать на частную жизнь людей. Однако не все уполномоченные по вопросам конфиденциальности в Канаде в настоящее время имеют право инициировать расследования или проверки при отсутствии жалобы, что может помешать им выполнять свою надзорную роль.[1412]

Таким образом, все уполномоченные по вопросам конфиденциальности должны иметь право инициировать и проводить расследования в отношении принятия полицией и использования технологий алгоритмического контроля.

Уполномоченные по правам человека на провинциальном и федеральном уровнях также играют важную роль в освещении вопросов прав человека, которые могут возникнуть с использованием алгоритмических технологий

[1412] Например, только мандаты уполномоченных по вопросам конфиденциальности и омбудсменов в Британской Колумбии, Альберте, Северо-Западном Нунавуте и Ньюфаундленде прямо предусматривают полномочия на возбуждение расследований или проверок государственных органов в отношении соблюдения применимого законодательства о конфиденциальности. Мандаты других провинций и территорий сосредоточены только на расследовании жалоб.

полицейского контроля. Правительства должны гарантировать, что эти органы оснащены адекватными ресурсами для выполнения этой задачи.[1413]Эта форма следственного обзора может происходить как процесс, основанный на жалобах, как форма рандомизированного аудита или как расследование, инициированное собственными силами уполномоченного в ответ на полученную информацию (например, детали, раскрытые в новостных отчётах или информацию, предоставленную стороной. это не истец).

Рекомендация 17: Правоохранительные органы должны принять и официально зафиксировать в письменной форме механизмы внутреннего надзора и подотчётности, передовой опыт и политику в отношении рассмотрения, разработки, закупок, использования, мониторинга, аудита и роспуска технологий алгоритмического полицейского контроля.

Правоохранительные органы должны создавать документацию и обеспечивать обучение в отношении любого использования технологии алгоритмической полицейской деятельности на каждом этапе, от первоначального рассмотрения до текущего аудита и потенциального расформирования, включения технологии алгоритмической полицейской деятельности в операции. Согласно исследованиям и интервью с представителями правоохранительных органов, формальность и документация политик различались между агентствами, участвующими в алгоритмической работе полиции. В некоторых случаях практики регулировались официальным протоколом совета по этике исследований, в то время как в других не существовало официальной документации, и казалось, что передовые методы являются результатом их отстаивания одним человеком. При введении в действие письменных правил правоохранительные органы должны сделать упор на преобразовании требований Хартии, разработанных в прецедентном праве, в чёткие письменные инструкции для непосредственных сотрудников.

Более того, от муниципальных начальников полиции следует потребовать, чтобы они публично представляли свои письменные правила своим надзорным советам и городским советам; все такие презентации должны быть открыты для публики, а не переноситься на закрытые собрания. Провинциальные и федеральные полицейские органы должны быть обязаны

[1413] См., например, Комиссия по правам человека Онтарио, A Collective Impact: Промежуточный доклад о расследовании полицией Торонто расового профилирования и расовой дискриминации чернокожих (November 2018). <http://www.ohrc.on.ca/en/public-interest-inquiry-racial-profiling-and- discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-and-racial-discrimination-black>; Office of the Privacy Commissioner of Canada, «Cell site simulators used by RCMP not capable of intercepting private communication», (September 2017), <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/>.

публиковать политику аналогичным образом; эта политика должна быть представлена либо министрами общественной безопасности, либо генеральными прокурорами, либо в законодательный орган, либо в соответствующий законодательный комитет. Эти политики должны быть представлены до любой реализации технологии алгоритмического контроля и любой новый класс технологий (например, модели прогнозируемого контроля на основе человека) должен быть явно и конкретно рассмотрен в этих планах.

Правоохранительным органам следует также принять и задокументировать механизмы проверки и аудита, включающие регулярный мониторинг и выборочные проверки журналов доступа к системе. В частности, эти механизмы будут сосредоточены на обнаружении необычного поведения и нарушений политик и процедур, регулирующих использование технологии алгоритмического контроля. Должностные лица будут уведомлены о том, что их деятельность подлежит аудиту или мониторингу и что их могут попросить оправдать использование системы.[1414]

В большинстве правоохранительных органов уже есть отделы внутренних профессиональных стандартов, которые рассматривают жалобы населения и проводят внутренние расследования.

Рекомендация 18: Правительствам следует выделить финансирование на исследования, чтобы получить независимые экспертные знания о последствиях алгоритмических полицейских технологий для прав человека.

Федеральные и провинциальные правительства должны предоставлять государственное финансирование отдельным лицам для развития экспертных знаний в области взаимосвязи алгоритмических технологий, уголовного правосудия и прав человека. Это финансирование должно включать, например, федеральное финансирование через Управление уполномоченного по вопросам конфиденциальности Канады, Совет естественных и инженерных исследований (NSERC) или Совет социальных и гуманитарных исследований (SSHRC). Если алгоритмические полицейские технологии и дальше будут использоваться в системе уголовного правосудия, надлежащая правовая процедура и права на судебную защиту, вероятно, будут затруднены на практике из-за отсутствия

[1414] В качестве примера процесса внутреннего аудита Комиссар по вопросам информации и конфиденциальности провинции Онтарио рекомендует полицейским службам провинции Онтарио внедрить регулярные процедуры аудита в отношении использования технологии автоматизированного распознавания номерных знаков: Комиссар по вопросам информации и конфиденциальности провинции Онтарио, "Руководство по использованию автоматизированных систем распознавания номерных знаков полицейскими службами", (July 2017), <https://www. ipc.on.ca/wp-content/uploads/2016/09/alpr_systems.pdf>.

доступных специалистов для проверки и оспаривания валидности алгоритмических методов. Области, подлежащие исследованию, должны включать общую надёжность алгоритма и любые используемые обучающие и эксплуатационные входные данные, методы обслуживания после того, как алгоритм был введён в действие, а также выходные данные алгоритма (например, тестирование на предмет произвольных или неточных результатов и эффективность инструмента по сравнению с неалгоритмическими методами).

Рекомендация 19: Правительства должны обеспечить предоставление адекватной помощи малообеспеченным и непредъявленным обвинением, чтобы привлечь свидетелей-экспертов в уголовном процессе.

Чтобы предъявить судьям иски о нарушениях прав человека об использовании алгоритмической полицейской технологии, обвиняемым потребуется доступ к экспертам, которые потенциально могут выступать в качестве свидетелей для оценки точности алгоритмических полицейских технологий. Во многих случаях обвиняемые не имеют права на юридическую помощь, но по-прежнему не могут нанять ни адвоката, ни экспертов. В случаях, когда обвиняемому не представлен адвокат, на суд и Королевского прокурора возлагаются повышенные обязанности по обеспечению доступа обвиняемого к справедливому судебному разбирательству. Правительствам следует предоставить финансирование организациям по оказанию юридической помощи, чтобы гарантировать, что технологи, представляющие общественные интересы, могут выступать в качестве свидетелей-экспертов. Это финансирование может быть выплачено из фондов юридической помощи, которые распределяются либо через процессы юридической помощи, либо, в качестве альтернативы, за счёт средств по распоряжению суда, предоставляемых для найма эксперта в случаях, когда обвиняемые не могут позволить себе нанять адвоката и не имеют прямого права на получение юридической помощи.

Помощь может также включать обучение прокуроров и судов Королевства по вопросам Хартии и вопросам доказывания, которые могут возникнуть в случаях, когда правоохранительные органы полагаются на технологию алгоритмического полицейского контроля.

Рекомендация 20: Правительства и правоохранительные органы должны по умолчанию сделать исходный код алгоритмических полицейских технологий общедоступным или, если это невозможно по соображениям общественного интереса, конфиденциально доступным государственным

органам и независимым экспертам для целей алгоритмической оценки воздействия, проверки перед закупкой, тестирования безопасности, аудита, расследования и судебных разбирательств.

Правительственные и правоохранительные органы, которые разрабатывают свои собственные алгоритмические технологии полицейского контроля – как внутри компании, так и с частными поставщиками, – должны сделать исходный код и связанные детали таких технологий общедоступными в машиночитаемых формах. Применение лицензирования открытого программного обеспечения в этом контексте может быть целесообразным на том основании, что такие технологии финансируются государством и должны быть доступны для общественности для целей обзора или исследования.[1415]

Если смягчающие обстоятельства затрагивают общественный интерес до такой степени, что перевешивает важность раскрытия исходного кода и связанных с ним деталей алгоритмических полицейских технологий для общественности, информация должна быть доступна для надзорных органов и независимых экспертов на конфиденциальной основе (если сам источник кода остаётся конфиденциальным, но выводы и решения являются общедоступными), чтобы завершить оценку воздействия.

Правительства и правоохранительные органы, которые приобретают готовые алгоритмические технологии полицейского контроля у коммерческих поставщиков, должны включать проверку открытого исходного кода в качестве условия всех контрактов на закупку, включая отказ от коммерческой тайны и связанных с ней прав собственности . Возможные агентства, которые могут играть надзорную роль в отношении обеспечения прозрачности, проверки, тестирования и аудита исходного кода, включают Управление уполномоченного по конфиденциальности и Канадский центр кибербезопасности.

6.6. Вывод

Технологии алгоритмической полицейской деятельности — это не просто выдумка или мнимые возможности. Они прибыли или прибывают в канадские города и провинции, и делают это быстро. Многие правоохранительные органы Канады использовали, разработали, закупили или протестировали ряд

[1415] Дополнительные сведения см. в разделе "IN FOCUS # 7: Open Source Algorithms and Source Code Review" в разделе 5.6.1 ("Информационные барьеры для надлежащей процедуры: алгоритмическая прозрачность и влияние частного сектора").

технологий алгоритмической полицейской деятельности. К ним относятся как алгоритмические технологии полицейского контроля, ориентированные на местоположение, так и ориентированные на человека (технологии «прогнозируемого полицейского контроля»), а также технологии алгоритмического наблюдения.

Общественные интересы требуют согласованного демократического участия и правовой реформы, нацеленной на использование алгоритмических полицейских технологий в системе уголовного правосудия. Канадские законодатели и правоохранительные органы должны извлечь уроки из юрисдикций, где такие технологии уже давно используются. В США полицейское управление Чикаго, полицейское управление Нового Орлеана и полицейское управление Лос-Анджелеса отказались от использования критикуемых алгоритмических полицейских технологий и закрыли несколько программ.[1416]Город Санта-Крус, Калифорния, в настоящее время рассматривает возможность полного запрета на все технологии прогнозирования полиции.[1417] Другие города, такие как Сан-Франциско и Окленд, Калифорния, Бостон и Сомервилл, Массачусетс, ввели моратории на использование технологий распознавания лиц. Независимые исследования и аудит технологий алгоритмической полицейской деятельности, используемых в Соединённых Штатах, продемонстрировали, что многочисленные риски и вред уже выявлены из-за относительно неконтролируемого использования инструментов алгоритмического наблюдения или развертывания ресурсов полиции на основе алгоритмических прогнозов, полученных на основе статистического анализа.[1418]

Воспроизведение, усиление или автоматизация методов полицейской деятельности прошлого с помощью полицейских алгоритмов ещё больше рискует укрепить враждебные, недоверчивые и антагонистические отношения

[1416] See e.g. Ali Winston, «New Orleans ends its Palantir predictive policing program", The Verge (15 March 2018) <https://www.theverge. com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end>; Jeremy Gorner & Annie Sweeney, «For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended", Chicago Tribune (24 January 2020), <https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html>; and Mark Puente, «LAPD to scrap some crime data programs after criticism", Los Angeles Times (5 April 2019) <https://www.latimes.com/local/lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html>.

[1417] Avi Asher-Schapiro, «In a U.S. first, California city set to ban predictive policing", Reuters (17 June 2020) <https://uk.reuters.com/article/ usa-police-tech/corrected-refile-feature-in-a-us-first-california-city-set-to-ban-predictive-policing-idUKL8N2DO3LD>.

[1418] Например, при объявлении о выводе из эксплуатации "Стратегического предметного списка" ДСП (алгоритмической технологии охраны порядка, ориентированной на человека) генеральный инспектор пояснил, что это решение было принято из-за "ненадежности оценок рисков и уровней; неправильно обученные присяжные; отсутствие механизмов контроля за внутренним и внешним доступом; вмешательства..., которые могут иметь негативные последствия для арестов, которые не привели к вынесению обвинительных приговоров; и отсутствие долгосрочного плана поддержания [моделей]": Sam Charles, «CPD decommissions 'Strategic Subject List'", Chicago Sun Times (27 January 2020), <https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson>.

между канадской правоохранительной системой и общественностью. Гражданские свободы и основные свободы ущемляются в ущерб, когда полиция неизбирательно использует эти технологии или когда такие технологии используются при отсутствии надлежащих конституционных гарантий. Баланс между задачами уголовного правопорядка и защитой основных свобод уже часто нарушается, когда речь идет о маргинализированных сообществах, особенно чернокожих и коренных сообществах. Внедрение алгоритмических полицейских технологий угрожает ещё больше подорвать гражданские свободы и основные свободы таких сообществ и их отдельных членов, ограничивая их человеческое достоинство и автономию, а также их способность в полной мере участвовать в общественной жизни или пользоваться равной защитой права.

Использование алгоритмических технологий в мощном аппарате полицейского надзора и правоохранительных систем может нанести реальный и значительный ущерб отдельным лицам и сообществам, увековечить несправедливость, уже отмеченную системой уголовного правосудия, и вызвать фундаментальную переориентацию методов полицейской деятельности, которые бросят вызов традиционному пониманию прав и средств правовой защиты, предусмотренных Хартией. Например, использование прогнозирующей полицейской технологии изменяет традиционные методы полицейской деятельности за счёт использования массивных исторических наборов полицейских данных таким образом, который никогда не предполагался участниками системы правосудия, в том числе теми, кто сформулировал текущие конституционные гарантии.

Использование технологий прогнозирования полицейской деятельности может подвергать людей усиленным подозрениям со стороны полиции, проверке, задержанию и т.д., основываясь не на собственных действиях человека, а на обобщениях, извлеченных из общих исторических закономерностей на уровне общины или страны. В качестве примеров технологий прогнозирования полиции в Канаде Департамент полиции Ванкувера (VPD) использует технологию алгоритмической полицейской деятельности, ориентированную на местоположение, связанную с их системой GeoDASH, в то время как Лаборатория прогнозной аналитики полиции Саскачевана (SPPAL) разрабатывает ориентированные на человека инструменты алгоритмической полицейской деятельности, которые предназначены для проведения оценки рисков для определения потенциальных жертв и потенциальных рецидивистов или насильственных преступников. Хотя каждая из этих программ включает встроенные меры, которые пытаются уменьшить вред и риски, указанные выше, они добровольно включили эти меры. Не все правоохранительные органы, применяющие алгоритмические или прогнозирующие технологии полицейского контроля, могут выбрать или

заранее реализовать адекватные меры безопасности. Таким образом, конституционные опасности и опасности для прав человека, связанные с такими технологиями, продолжают угрожать Канаде. Основные права человека и гражданские свободы не могут быть оставлены на усмотрение местных правоохранительных органов. Другие полицейские службы Канады также могут использовать или развивать технологии прогнозирования полицейской деятельности вне пределов осведомленности общественности. Многие из запросов о свободе информации, представленных для этого отчёта, были встречены ответами правоохранительных органов, которые утверждали, что привилегия является оправданием неразглашения. В других случаях правоохранительные органы не ответили на поданный запрос о свободе информации. Авторы этого отчёта также ранее подали запрос о свободе информации в TPS, который включал широкий запрос записей, касающихся распознавания лиц, в течение периода времени, начиная с марта 2018 года. TPS не предоставил никакой информации или соответствующих документов относительно использования распознавания лиц, несмотря на тот факт, что теперь известно, что полицейская служба потратила 451 718 долларов на систему распознавания лиц в течение периода времени, который был предметом запроса о свободе информации.[1419] Некоторые правоохранительные органы в настоящее время не участвуют в прогнозировании полицейской деятельности, но они уже оснащены технологическими возможностями для этого или могут рассмотреть вопрос об участии в будущем. Например, полицейская служба Калгари (CPS) имеет возможность проводить ориентированную на человека прогнозирующую полицейскую работу с помощью своего программного обеспечения Palantir Gotham, хотя сотрудник правоохранительных органов в Калгари заявил, что в настоящее время система используется только для неалгоритмического управления и анализа данных. В 2018 году в статье представителя Environics Analytics, который сотрудничает с TPS по инициативам в области полицейского контроля на основе данных, говорится, что одной из целей сотрудничества организаций является разработка алгоритмических моделей, которые будут определять области, считающиеся «высокопреступными». Согласно результатам исследования, проведённого в ходе интервью для этого отчёта, TPS в настоящее время не занимается алгоритмической прогнозирующей политикой и не намеревается немедленно внедрять технологии прогнозирующей полиции. Однако эта позиция не исключает возможности того, что TPS может рассмотреть вопрос о том, чтобы сделать это в будущем, и агентство заинтересовано в использовании данных для информирования полицейских решений о преступлениях против собственности и насилия с применением огнестрельного оружия.

[1419] Phillip Lee-Shanok, «Privacy advocates sound warning on Toronto police use of facial recognition technology», CBC News (30 May 2019), <https://www.cbc.ca/news/canada/toronto/privacy-civil-rights-concern-about-toronto-police-use-of-facial-recognition-1.5156581>.

Технологии алгоритмического наблюдения, описанные в этом отчёте, также рискуют вызвать сейсмические изменения в способах мониторинга и наблюдения за населением в Канаде правоохранительными органами. Канадские правоохранительные органы полагаются на несколько различных видов таких технологий. Технология распознавания лиц, автоматические считыватели номерных знаков и программное обеспечение для наблюдения в социальных сетях были внедрены многочисленными правоохранительными органами по всей стране. Алгоритмическая обработка позволяет правоохранительным органам принципиально по-новому использовать данные, которые ранее собирались на относительно безальтернативной или нерегулируемой основе или разрешалось собирать без учёта сегодняшних технологических реалий (например, когда базы данных снимков или видеозаписи с камер видеонаблюдения, содержащие собранные данные при прежних режимах использования технологии распознавания лиц в правоохранительных целях). Технология алгоритмического наблюдения имеет тенденцию собирать и анализировать личную информацию из общественных мест, например, на открытом воздухе, на публичных мероприятиях, таких как массовые протесты или в онлайн-среде. Перспектива дальнейшего разрастания сферы, в которой полиция может без разбора наблюдать за представителями общественности, должна вызывать серьезную озабоченность, особенно если эти технологии не подвергаются необходимым ограничениям и механизмам надзора.

Технология распознавания лиц, похоже, быстро внедряется канадскими правоохранительными органами. Инструмент NeoFace Reveal корпорации NEC в настоящее время используется CPS и был протестирован в начале 2019 года полицейской службой Оттавы. TPS также использует технологию распознавания лиц, которая представляет собой либо NeoFace Reveal, либо другой продукт корпорации NEC. Более того, сообщения СМИ в начале 2020 года показали, что спорный инструмент распознавания лиц Clearview AI использовался или тестировался всеми RCMP, CPS, Полицейской службой Эдмонтона и несколькими полицейскими службами Онтарио, включая TPS и службы в Пил, Халтон, Оттава, Дарем, Ниагара и Гамильтон. Учитывая очевидные риски для прав человека, связанные с инструментами распознавания лиц, в дополнение к их ненадёжности, полицейские службы должны прекратить любое дальнейшее использование или внедрение технологий распознавания лиц до тех пор, пока не будут приняты соответствующие законы и правила и такие инструменты не будут продемонстрированы в соответствии с предварительными условиями надёжности, необходимости и соразмерности.

Правоохранительные органы Канады также широко занимаются слежкой в социальных сетях. В настоящее время RCMP использует программное обеспечение для мониторинга социальных сетей, известное как Social Studio,

предоставляемое Carahsoft и разработанное Salesforce. В апреле 2020 года RCMP также объявил открытый тендер на поиск ещё более сложных сервисов наблюдения за социальными сетями, чем те, которые уже используются, несмотря на продолжающийся внутренний анализ законности его текущих операций по наблюдению за социальными сетями. И CPS, и TPS в прошлом проводили алгоритмическое наблюдение за социальными сетями, используя инструмент Media Sonar, созданный компанией в Лондоне, ON. Оба полицейских ведомства прекратили использовать это программное обеспечение после того, как Twitter и Facebook запретили его использование на своих платформах (включая Instagram), поскольку Media Sonar продвигал использование своей технологии для нацеливания на социальные движения, такие как Black Lives Matter. Кроме того, CPS занимается алгоритмическим анализом социальных сетей, используя систему, которая импортирует сетевые реляционные данные из программного обеспечения Palantir в IBM i2 Analyst Notebook, чтобы идентифицировать ключевых игроков в данных социальных сетях. Механизмы подотчётности и надзора имеют решающее значение для приведения использования этих технологий в конституционные рамки и для защиты прав на свободу выражения мнений, равенство и неприкосновенность частной жизни, которые подрываются алгоритмическим полицейским надзором и мониторингом в онлайновой, наружной или иной общественной среде. Более того, правоохранительные органы, похоже, используют дополнительные технологии способами, которые нарушают более традиционные конституционные границы. В частности, этот отчёт раскрыл информацию, позволяющую предположить, что провинциальная полиция Онтарио и региональная полицейская служба Ватерлоо могут незаконно перехватывать личные сообщения в частных онлайн-чатах с использованием другой формы технологии наблюдения за социальными сетями, известной как Система защиты ребенка в Интернете (ICACCOPS).[1420]

Хотя алгоритмические полицейские технологии остаются новой проблемой для канадской правовой системы, аналогичные уроки уже были извлечены в системе уголовного правосудия в результате системных сбоев, проистекающих из несовершенных новых научных, технологических или следственных методов. Использование «ошибочных процедур судебно-медицинской экспертизы, ненадёжных научных данных и ошибочных заключений экспертов было факторами в ряде дел о неправомерном осуждении в Канаде», [1421]которые привели к многочисленным публичным запросам, направленным на выявление и установление методов предотвращения

[1420] See discussion of the ICACCOPS tool and related legal analysis in Section 4.3.2 («Social Media Surveillance»).

[1421] Public Prosecution Service of Canada, «Prevention of Wrongful Convictions», Public Prosecution Service of Canada Deskbook (September 2014), <https://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/tpd/p2/ch04.html#fnb37-ref>.

повторяющихся сбоев.[1422] Эти расследования неоднократно подчёркивали необходимость крайней осторожности, когда дело доходит до использования новых или непроверенных методов в системе уголовного правосудия.

Оценка алгоритмических полицейских технологий через призму прав человека показала, как их использование правоохранительными органами может вызвать множество нарушений гражданских свобод в соответствии с конституцией Канады и международным правом прав человека. В частности, использование алгоритмических технологий полицейского контроля серьёзно угрожает следующим правам человека:

- право на неприкосновенность частной жизни (через такие проблемы, как неизбирательное наблюдение, подрыв разумных ожиданий конфиденциальности в публичных и сетевых пространствах, точность выводных данных и обмен данными между правоохранительными органами и другими государственными органами);
- право на свободу выражения мнений, мирных собраний и объединений (через такие проблемы, как подрыв анонимности толпы и нацеливание на социальные движения и маргинализованные сообщества);
- право на равенство (через такие проблемы, как алгоритмическая предвзятость, увековечивающая дискриминационные петли обратной связи, повышенная видимость данных о социально-экономически неблагополучных лицах и систематическая дискриминация,, ограничивающая возможности структурной реформы для решения основных проблем);
- право на свободу и свободу от произвольного задержания (через такие проблемы, как обобщённые статистические выводы, заменяющие индивидуальные подозрения, и риски предвзятости автоматизации);
- право на надлежащую правовую процедуру и средство правовой защиты (через такие проблемы, как отсутствие прозрачности, подотчётности и механизмов надзора, таких как требования об уведомлении и раскрытии информации).

Среди многочисленных проблем, связанных с Конституцией и правами человека, которые были выявлены в этом отчёте, возникло несколько особенно заметных опасностей, которые демонстрируют фундаментальную несовместимость между использованием алгоритмических полицейских технологий и конституционной защитой и защитой прав человека. Эти несовместимости – яркий красный свет, на который должны обратить внимание правоохранительные органы, участники системы правосудия и политики: если

[1422] The Hon. Commissioner Stephen T. Goudge, Inquiry into Pediatric Forensic Pathology in Ontario (Toronto, 2008); The Hon. Justice Cory, The Report of the Commission of Inquiry regarding Thomas Sophonow (September 2001), <https://digitalcollection.gov.mb.ca/awweb/ pdfopener?smd=1&did=12713&md=1>; The Hon. Fred Kaufman, C.M., Q.C., Report of the Kaufman Commission on Proceedings Involving Guy Paul Morin (1998).

они не будут руководить курсом правосудия, чтобы избежать этих предательских скал, историческое неравенство будет продолжаться или ухудшаться, а канадская система правосудия в лучшем случае будет поставлена под сомнение, а в худшем – обречена на откровенную дурную репутацию. Чтобы смягчить наиболее вредные правовые и политические последствия, связанные с алгоритмическими полицейскими технологиями, система уголовного правосудия должна принимать во внимание, в частности, следующие три проблемы.

Во-первых, систематическая предвзятость и искаженные данные в исторических наборах полицейских данных представляют особенно серьёзную проблему для алгоритмических технологий, ориентированных на человека и местоположение. Такого рода инструменты алгоритмического контроля позволяют прогнозировать, кто совершит уголовное преступление, насколько вероятно, что кто-то совершит уголовное преступление в течение определённого времени или где и когда могут иметь место определённые виды уголовных преступлений. Если все наиболее распространенные источники исторических данных полиции содержат систематическую предвзятость и неточности, целостность алгоритмических выходных данных, полученных с использованием этих данных, будет также поставлена под угрозу. В результате в этом отчёте подчёркивается необходимость моратория на использование исторических данных полиции при обучении или использовании полицейских алгоритмов, а также необходимость одновременного проведения судебного расследования такого использования. В тех случаях, когда общины подвергались дискриминационному обращению на основании закрепленных в Хартии оснований, собранные о них данные должны считаться непригодными для использования в алгоритмах обучения, которые используются в полиции для принятия решений.

Во-вторых, использование прогностических форм алгоритмических технологий полицейского контроля или ненадёжных алгоритмических технологий наблюдения для оправдания посягательства на свободу человека (например, путём ареста или задержания) несовместимо с конституционным законодательством и законодательством о правах человека. Алгоритмические прогнозы по своей природе обобщены в той степени, в которой они не отвечают требованиям конкретной и индивидуальной подозрительности, чтобы оправдать посягательство на свободу человека. Эта фундаментальная несовместимость между алгоритмическими полицейскими технологиями и правом на свободу должна исключать использование таких технологий в большинстве, если не во всех, непосредственных полицейских работах, чтобы предотвратить случаи задержаний, арестов или обвинений на неконституционных основаниях, полученных из алгоритмических прогнозов или иным образом.

В-третьих, всё более широкое использование технологий алгоритмического наблюдения правоохранительными органами Канады ставит под угрозу право на неприкосновенность частной жизни и защищенные Хартией основные свободы выражения мнений и ассоциаций. В правовой системе Канады в настоящее время отсутствуют достаточные гарантии для обеспечения того, чтобы методы алгоритмического наблюдения соответствовали конституционным требованиям и подпадали под действие надёжных и необходимых механизмов регулирующего, судебного и парламентского надзора. Неограниченное использование технологий алгоритмического наблюдения имеет огромный потенциал, чтобы нанести ущерб способности осуществлять основные свободы и гражданские свободы, тем самым подрывая свободное и демократическое общество. В сочетании с отсутствием механизмов надзора и подотчётности, включая соблюдение ограничений, установленных принципами необходимости и соразмерности, использование таких технологий в настоящее время не имеет юридического обоснования.

В заключение, правовой анализ и обзор неадекватных систем надзора Канады в этом отчете демонстрируют, что подавляющее большинство изученных алгоритмических технологий полицейского контроля не должны использоваться какими-либо канадскими правоохранительными органами. Теоретически могут существовать очень узкие и специфические области применения технологий алгоритмической полицейской деятельности, которые явно не нарушают конституционный закон и законы о правах человека, если даже они достаточно надёжны для использования. Однако чрезвычайно сложно определить, какими могут быть эти редкие технологии или варианты использования без публичной прозрачности и исчерпывающей информации от правоохранительных органов, которая включает подробное раскрытие информации о том, какие технологии они рассматривают, разрабатывают или внедряют; прошли ли какие-либо такие технологии независимую научную проверку; и как любые такие технологии будут использоваться и регулироваться внутри страны. Тем не менее, в его нынешнем виде существует множество тревожных сигналов, которые предупреждают о значительной опасности в будущем для правительств, полицейских служб и, прежде всего, общественности и членов исторически маргинализованных сообществ, которые понесут на себе основную тяжесть негативных последствий, связанных с использованием алгоритмических полицейских технологий. Именно по этой причине в части 6 излагается краткий список приоритетных рекомендаций, в которых подчёркивается необходимость целевых мораториев и чётких ограничений в отношении наиболее проблемных видов использования алгоритмических полицейских технологий с точки зрения Конституции и прав человека. Именно по этой причине в данном отчёте подчёркивается

необходимость конструктивных консультаций и выслушивания исторически маргинализированных сообществ, на которых непропорционально влияет канадская система уголовного правосудия, при определении того, как двигаться вперёд с внедрением алгоритмических полицейских технологий в Канаде.

Что касается маргинализированных сообществ, которые исторически подвергались системной дискриминации в системе уголовного правосудия, алгоритмические полицейские технологии вызывают серьёзные вопросы, касающиеся их коллективных интересов и прав. В данном отчёте основное внимание уделяется ситуациям, в которых гражданские свободы или права человека могут быть нарушены с помощью таких технологий. Однако, если на человека пагубно воздействует технология алгоритмической полицейской деятельности в силу его принадлежности к группе, имеющей защищенную территорию согласно разделу 15, и из-за социально-политического и исторического контекста чрезмерного контроля этой группы в Канаде, такая технология также поднимает вопросы о его материальном и системном воздействии на коллективную неприкосновенность частной жизни, свободу и равноправие этого сообщества в целом. Таким образом, индивидуальных средств правовой защиты может оказаться недостаточно, если оскорбительное воздействие технологий алгоритмической полицейской деятельности является как распределительным, так и коллективным, но при этом сосредоточено в определенных сообществах, которые в прошлом подвергались системной дискриминации. Взаимосвязь между индивидуальными и коллективными правами человека в отношении исторически маргинализированных сообществ и, в частности, роль права на равенство, поскольку оно пересекается с другими средствами защиты Хартии, требует дальнейшего изучения в рамках исследовательских расследований и должна быть изучена в рамках рекомендованного судебного расследования.[1423]

Учитывая бесчисленное множество опасностей, которые технологии алгоритмического контроля представляют для прав человека, весьма сомнительно, оправдывают ли такие технологии свои существенные затраты (в сфере закупок, разработки, тестирования, внедрения, мониторинга, аудита и защиты от проблем, связанных с их использованием или результатами). Технологии алгоритмической полицейской деятельности также будут происходить за счёт отвлечения дальнейшего финансирования и государственных ресурсов от более насущных приоритетов в пользу затронутых сообществ и более эффективных подходов к безопасности сообществ. По всей стране поднимается множество вопросов относительно надлежащей роли полицейских служб, и растёт признание того, что масштабы и

[1423] See e.g., Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, Group Privacy: New Challenges of Data Technologies (Cham, Switzerland: Springer International Publishing, 2017

бюджет полицейской деятельности значительно выросли и не соответствуют таким областям, как лечение психических заболеваний, консультирование, благополучие учащихся. В этом отчёте также обсуждается связь между основными факторами маргинализации и тенденцией к несоразмерной криминализации и несправедливому и ненужному вовлечению в систему уголовного правосудия. Алгоритмические полицейские технологии ничего не сделают для устранения коренных причин социальных проблем, которые систематически и пагубно связаны с системой уголовного правосудия, включая бездомность, неадекватные услуги в области психического здоровья и наркозависимости, недостаточное финансирование систем образования, неадекватные общественные ресурсы для поддержки борющейся молодёжи и предотвращения насилия, отсутствие медицинского обслуживания, безработица или наследие канадского колониализма и связанные с ним травмы, передаваемые из поколения в поколение. Любой анализ алгоритмических полицейских технологий должен начинаться с оценки их воздействия на конституционные права и права человека. В этом отчёте показано, что некоторые виды использования и некоторые типы таких технологий в корне несовместимы с Канадской хартией прав и свобод, поэтому в значительной степени не имеет значения, является ли технология надёжной или даёт ощутимую пользу для целей правоохранительных органов. Канадское правительство и правоохранительные органы имеют конституционный императив учитывать и предотвращать вред, который может возникнуть в результате дальнейшего закрепления существующих дискриминационных моделей полицейской деятельности и лишения свободы, особенно в отношении исторически маргинализированных сообществ, защищаемых разделом 15 Хартии. Какими бы ни были интересы правоохранительных органов в доступе к возможностям алгоритмических полицейских технологий, этот интерес не имеет и не должен преобладать над основными правами и свободами, которые конституция гарантирует каждому человеку, включая права на неприкосновенность частной жизни, равенство и свободу. и этот интерес не должен иметь приоритет над ценностями, которые такие права и свободы отстаивают по своей сути, такими как человеческое достоинство и автономия. Последовательные расследования и обзоры подчёркивают, что правоохранительные органы и правительство Канады в целом должны действовать, чтобы устранить неравенство в системе уголовного правосудия и во всём обществе в целом, особенно в отношении исторически маргинализированных и бесправных лиц и групп, которые наиболее глубоко и несправедливо пострадали. Призывы к выполнению этой работы не новы и не являются новой реакцией на достижения в области полицейских технологий. Переход к технологиям алгоритмической полицейской деятельности - будь то массовое наблюдение, прогнозирование преступности или оценка рисков отдельных лиц - или иное дальнейшее закрепление модели полицейской

деятельности с использованием «больших данных» в Канаде рискует ещё больше увековечить уровни системной дискриминации в системе уголовного правосудия до ещё большего и потенциально необратимая степень. Такое увековечение могло бы произойти, несмотря на широкий консенсус, достигнутый среди органов надзора за системой правосудия, и признание общественностью необходимости положить конец непропорциональной полицейской деятельности и тюремному заключению общин, которые были объектами исторической и продолжающейся системной дискриминации, в том числе чернокожих и коренных народов, частных лиц.

Вместо того, чтобы компенсировать чрезмерную полицейскую деятельность и тюремное заключение, алгоритмические полицейские технологии могут вместо этого безвозвратно кодировать дополнительные уровни неравенства и дискриминации в системе уголовного правосудия. Такие технологии могут, в то же время, замаскировать эту несправедливость, сохраняя тонкий слой математической «нейтральности». Какие бы скромные выгоды алгоритмические полицейские технологии теоретически ни принесли правоохранительным органам, вместо этого следует направить государственные ресурсы на устранение коренных причин несправедливости, исследуемых через призму пересекающихся основанных на фактах выработки политики, и на прекращение наследия предотвратимых трагедий, угнетения и системного ущерба, что нашло отражение в истории канадской системы уголовного правосудия.

Приложение A. Образец запроса о свободе информации

Дата

Имя

Заголовок

Уважаемый [сотрудник FOI или ATIP],

Я пишу, чтобы подать запрос на записи в соответствии с разделами 4 (1) и 6 Закона Канады о доступе к информации, R.S., 1985, c. a-1. В частности, я прошу следующее:

1. **Все записи,** включая, помимо прочего, черновую и окончательную версии политики, руководящие принципы, повестки дня собраний, протоколы собраний или заметки, информационные заметки, технические спецификации,

учебные документы, бюллетени, меморандумы, резюме, слайды, раздаточные материалы, рукописные заметки, подготовительные заметки, заметки из телефонных звонков, факсы, отчеты, диаграммы, исследования, обзоры, контракты, бюджеты, финансовые документы, и вся внутренняя и внешняя корреспонденция, включая электронную почту отправленную в период с 1 января 2013 г. по 1 ноября 2018 г., которая содержит обсуждение или ссылку на использование:

- **Алгоритмы, алгоритмическое принятие решений, алгоритмическая аналитика, алгоритмический анализ или автоматический анализ;**
- **Алгоритмическая оценка риска или алгоритмический анализ риска;**
- **Предиктивная аналитика, предиктивный анализ, предиктивное моделирование, предиктивный интеллект;**
- **Машинное обучение, глубокое обучение, нейронные сети, искусственный интеллект, «большие данные» или интеллект, управляемый данными;**
- **Мониторинг социальных сетей, аналитика социальных сетей;**
- **Распознавание лиц.**

В целях сбора, управления, анализа или оценки данных и информации, связанных с мониторингом, расследованием или реагированием на преступную деятельность, подозреваемую преступную деятельность и/или прогнозируемую преступную деятельность.

Все записи, включая, помимо прочего, предварительные и окончательные версии политик, руководящих принципов, повесток дня заседаний, протоколы заседаний или заметки, информационные заметки, технические спецификации, учебные документы, бюллетени, меморандумы, резюме, слайды, раздаточные материалы, рукописные заметки, подготовительные заметки, заметки из телефонных звонков, факсов, отчетов, диаграмм, исследований, опросов, контрактов, бюджетов, финансовых документов, а также всей внутренней и внешней корреспонденции, включая электронную почту, – подготовленные **в период с 1 января 2013 г. по 1 ноября 2018 г.,** которые содержат обсуждение или ссылку на использование:

- **Алгоритмы, алгоритмическое принятие решений, алгоритмическая аналитика, алгоритмический анализ или автоматический анализ;**

- **Алгоритмическая оценка риска или алгоритмический анализ риска;**
- **Предиктивная аналитика, предиктивный анализ, предиктивное моделирование, предиктивный интеллект;**
- **Машинное обучение, глубокое обучение, нейронные сети, искусственный интеллект, «большие данные» или интеллект, управляемый данными;**
- **Мониторинг социальных сетей, аналитика социальных сетей;**
- **Распознавание лица.**

Для целей определения правонарушителя или подозреваемого правонарушителя, обвиняемого, подсудимого, заключенного или осужденного, в том числе, помимо прочего, в целях исправительных услуг, заключения под стражу, освобождения под залог, вынесения приговора, классификации безопасности заключённого, оценки риска или условно-досрочного освобождения.

3. Все записи, включая, помимо прочего, предварительные и окончательные версии политик, руководящих принципов, повесток дня заседаний, протоколы заседаний или заметки, информационные заметки, технические спецификации, учебные документы, бюллетени, меморандумы, резюме, слайды, раздаточные материалы, рукописные заметки, подготовительные заметки, заметки из телефонных звонков, факсов, отчётов, диаграмм, исследований, опросов, контрактов, бюджетов, финансовых документов, а также всей внутренней и внешней корреспонденции, включая электронную почту, – подготовленные **в период с 1 января 2013 г. по 1 ноября 2018 г.,** которые содержат обсуждение или ссылка на любое из следующего:

- **Предиктивная полиция**
- **Проактивное наблюдение**
- **Полиция под руководством разведки**
- **Алгоритмический контроль**
- **Контроль за большими данными**
- **Предсказание криминальных «горячих точек»**
- **Алгоритмы контроля**
- **Доказательная деятельность полиции**
- **Проактивное патрулирование**

Если возможно, отправляйте значимую часть ответов на любой из вышеперечисленных пунктов сразу после их завершения, а не дожидаясь, пока будет собрана вся информация для всего этого запроса.

Если для получения полного ответа потребуется более тридцати дней, пожалуйста, отправьте в качестве первоначального промежуточного раскрытия список документов, которые будут раскрыты в ответ на запрос.

Я бы предпочёл получать все записи в электронном виде в читаемом компьютерном формате. Пожалуйста, отправьте их по электронной почте на следующие два адреса:

cynthia@citizenlab.ca

yolanda.song@utoronto.ca

Пожалуйста, не стесняйтесь обращаться ко мне, если необходимы какие-либо разъяснения или если они помогут выполнить или ускорить ответ на этот запрос. Буду рад продолжить обсуждение и помочь.