ПРЕДМЕТ СОЦИОЛОГИЧЕСКОГО АНАЛИЗА И РЕАЛИЗАЦИЯ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЙ В ПРАКТИКЕ ОБЕСПЕЧЕНИЯ РАЗЛИЧНЫХ СЛАГАЕМЫХ БЕЗОПАСНОСТИ СОВРЕМЕННОГО СОЦИУМА

Комлев Ю.Ю.,

доктор социологических наук, профессор
Казанский юридический институт МВД России

Проблемы и меры цифрового социального контроля в «Обществе наблюдения»

Мир настоящего ярко заявил о себе новым технологическим укладом. Цифровые технологии, смартфоны, компьютеры и другие «умные» девайсы радикально преобразовали жизнь людей в начале XXI века. В работах современных теоретиков (М. Кастельса, Д. Лаптон, Ш. Браун, М. Яр, К. Хейворда, Г. Страттона, Н. Селвина, Я. Гилинского, В. Овчинского и др.) феноменология таких цифровых перемен, как цифровое неравенство, киберпреступность и кибервиктимзация рассматривается в контексте сплетения «человечности, материальности и дигитальности». Впрочем, на связь технологий и социальных сдвигов пристальное внимание обращали и классики социологии (О. Конт, Г. Спенсер, Э. Дюркгейм, Т. Парсонс, Р. Мертон, Т. Веблен, У. Ростоу, Д. Бэлл, А. Тоффлер и др.). В первой четверти XXI века с развитием и внедрением во все сферы жизни людей интернета, цифровых технологий и систем цифровой связи, с моей точки зрения, сложились новые измерения социума постмодерна: цифровизация и сетевизация[1].

Цифровой мир со своими технологиями открывает не только новые возможности для человека, общества и государства, но и порождает различные социальные проблемы, в том числе массовую кибердевиантность, киберпреступность, кибервиктимизацию. Палитра форм кибердевиантности постоянно расширяется. Среди них: сетевая зависимость с утратой навыков реального общения; бегство от действительности в мир виртуальных симуляций (эскейпизм/эскапизм); киберлудомания (игровая зависимость); кибербуллинг (травля в интернете, социальных сетях, мессенджерах), кибергруминг (виртуальные сексуальные домогательства и насилие над несовершеннолетними); компьютерная педофилия; интернет-торговля наркотиками; пропаганда ненависти и распространение экстремистских идей, фишинг, вовлечение подростков и простаков

[1] Подр.: Комлев Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии // Российский девиантологический журнал. 2022. Т. 2. № 1. С. 17-26.

в террористическую деятельность или в финансирование неприятеля на фронтах СВО. Киберпреступники постоянно совершенствуются, умело разыгрывая драмы и другие постановки перед своими жертвами. Они, управляя процессом впечатлений, успешно добиваются в итоге реализации своих преступных целей по технологии, которую описал еще И. Гофман в середине прошлого века.

Продолжается стремительный рост регистрируемой киберпреступности: в 2022 г. совершено каждое четвертое, в 2023 г. – каждое третье преступление с использованием информационно-телекоммуникационных технологий (ИКТ). В 2024 г. в целом по стране зарегистрировано 40 % киберпреступлений в форме мошенничества. Тенденция, заключающаяся в высоких темпах роста киберпреступности, скорее всего, сохранится, поскольку в киберпространстве институты правопорядка не могут в полной мере реализовать принцип неотвратимости наказания, а барыши от высокотехнологичной преступности существенно превышают доходы от обычных краж, разбоев и других форм «уличной преступности»[1]. В ответ на изменения в формах совершения преступлений в цифровой среде и другие цифровые вызовы, дезорганизующие социальный порядок, формируются и новые практики цифрового социального контроля[2].

Обзоры теоретических положений и опыта социального контроля на рубеже XXI века показали, что предтечей цифрового социального контроля в настоящее время были постепенные сдвиги в сторону структурно-средового противодействия группам криминального риска. В этом русле сформировались положения «новой пенологии» по регулированию уровня девиаций, а не прерывания девиантной активности (М. Фили, Д. Саймон). В частности, исследователи предлагали в меньшей степени поднимать вопросы ответственности, вины, вмешательства в девиантную активность на индивидуальном уровне, но существенно большую роль отводить методикам идентификации, классификации и управления группами, выделяемыми по признаку криминальной опасности. В 90-е годы прошлого века сформировался переход в системе социального контроля от «надзора» к «слежению» или мониторингу (Т. Дамм). Мир постмодерна – это «общество контроля» (Ж. Делез), в котором речь больше идет не об «аресте и возвращении преступника к нормальной жизни» после совершения им преступления, а об осуществлении слежения за действиями индивидов, представляющих опасность, что позволяет

[1] Подр.: Комлев Ю.Ю. Указ. соч.

[2] Подр.: Комлев Ю.Ю. От цифровизации социума и киберпреступности к подготовке киберполицейских // Вестник экономики, права и социологии. 2025. № 2. С. 378-382.

принимать упреждающие меры. В первой четверти XXI века по итогам очередной научно-технической революции цифровые технологии привели к формированию «общества наблюдения»[1].

Обобщения автора с учетом выводов из работ L. Khalil, В. Овчинского, Т. Шипуновой, Я. Гилинского и др. позволяют уточнить ряд мер, тенденций и проблем в сфере трансформации социального контроля в цифровую форму в «обществе наблюдения». Наиболее важные из них тезисно состоят в следующем.

1. Постоянный, нарастающий объем и совершенствование использования цифровых видеокамер и биометрических наблюдений в общественных пространствах, основанных на технологии распознавания лиц.

2. Развитие интеллектуальных систем фиксации и цифровой идентификации отпечатков пальцев, рисунков сетчатки и радужной оболочки, голосовых паттернов и других идентификаторов.

3. Использование алгоритмических решений с помощью аналитики Big Data и искусственного интеллекта для мониторинга за девиантами. Накапливается опыт применения искусственного интеллекта для быстрого принятия типовых судебных решений.

4. Совершенствование контроля по рестрикции свободного доступа к информации в Интернете (ограничения с помощью блокировки адреса интернет-протокола («IP»), системной («DNS») фильтрации. Китай и Россия, Бразилия и Турция, другие страны принимают законы, направленные на создание национального, автономного интернета.

5. Меры обеспечения кибербезопасности в «обществе наблюдения» интерпретируются как «цифровой авторитаризм», как инструмент «контроля, подавления и манипуляций» в интересах государства. Практики цифрового контроля над киберпреступностью нередко распространяются на гражданские и политические права.

6. Совершенствуется наблюдение в социальных сетях за онлайн-активностью и персональными данными отдельных лиц из «проблемных» групп, пропагандирующих экстремизм и террор, вовлечение в самоубийство. Развиваются сложные методы фильтрации контента, которые используют алгоритмы, основанные на машинном обучении (искусственный интеллект).

7. Девиантологи и юристы справедливо отмечают отставание в развитии формального (правового) социального контроля в цифровой сфере. Это относится и к совершенствованию международного законодательства, которое на данный момент сводится в основном к

[1] Подр.: Комлев Ю.Ю. Социальный контроль в VUCA-мире и «обществе наблюдения»: состояние, тренды и этические проблемы // Вестник экономики, права и социологии. 2022. № 2. С. 114-116.

Будапештской конвенции Совета Европы о компьютерных преступлениях (2001 г.) и национальному законодательству.

8. Информационная политика России в области использования цифровых технологий направлена на повышение сервисных функций в предоставлении государственных услуг и защиты данных. Однако нормативная база, фиксирующая принципы и нормы правового регулирования в этой сфере, определяется ФЗ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», положения которого определенно нуждаются в коррекции. В 2016–2017 годы приняты Доктрина информационной безопасности РФ и Стратегия развития информационного общества в России на 2017–2030 годы, разработаны и реализуются национальные программы «Информационное общество» (2014), «Цифровая экономика РФ» (2019), где есть федеральный проект «Информационная безопасность».

9. Запаздывает институциализация полицейских структур по борьбе с киберпреступностью (киберполиция). В Китае с 2015 года образована «сетевая полиция». В структуре МВД России киберполиция создана (по отраслевому принципу) только 11 ноября 2022 года – Управление по организации борьбы с противоправным использованием информационно-коммуникативных технологий.

10. Исследователи и практики обращают внимание на необходимость повышать «цифровую грамотность» населения, чтобы снизить кибервиктимизацию, развивать культуру безопасности при использовании цифровых технологий. В МВД РФ по линии киберполиции ведется работа по информированию цифровых пользователей, например через дзен-канал (Вестник Киберполиции России), где раскрываются способы совершения киберпреступлений, формулируются правила цифровой гигиены. Пора, начиная с детства, готовить «цифровых граждан», адаптированных к использованию возможностей цифровых технологий с защитой от их опасных последствий в киберпространстве.

11. Развивается гибридизация социального контроля как сочетание формального и неформального контроля с использованием цифровых инструментов. Например, неравнодушные люди обращают внимание на парковку автомобилей в неустановленных местах: на тротуарах, газонах. Подобный факт фиксируется очевидцем с помощью цифровой камеры, а файл с номером, маркой транспортного средства, датой, местом нарушения (фото) направляется в рамках ГИС «Народный инспектор» в местный общественный пункт охраны порядка для разбора и вынесения административного решения.

12. В совершенствовании системы цифрового социального контроля чрезвычайно важны не только совершенствование законода-

тельства, мер и практик его применения, развитие цифрового гражданства и самоконтроля, но и подготовка квалифицированных специалистов по кибербезопасности в целом и особенно в сфере правоохранительной деятельности. Реализация государственной информационной политики в рамках федерального проекта «Информационная безопасность» приближает нас к решению этой кадровой проблемы. Опыт стран с высоким уровнем цифровизации и сетевизации социума показывает, что там создаются и развиваются факультеты, кафедры, образовательные программы, как правило магистратуры, по подготовке междисциплинарных специалистов по кибербезопасности.

В нашей стране готовят специалистов либо по техническим направлениям подготовки («Безопасность информационных технологий в правоохранительной сфере» – 10.05.05; «Информационная безопасность» – 10.03.01), либо по юридическому направлению («Правовое обеспечение национальной безопасности» – 40.05.01) с профилизацией по розыску преступников и расследованию киберпреступлений. Для правоведа, специализирующегося в сфере кибербезопасности расследования киберпреступлений, необходимы фундаментальные знания, умения и навыки в области цифровых технологий; передачи, хранения и обработки цифровой информации; методологии защиты цифровой информации; криптографии; электронной коммерции; кибердевиантности и киберпреступности; документирования цифровых следов преступлений против личности и др. Успеху в решении кадровых проблем ОВД будут способствовать как новые образовательные программы, обеспечивающие добротную цифровую подготовку киберполицейских, так и преодоление системного обесценивания труда полицейских в последние 10 лет. Это по-прежнему стратегически значимая профессия, развивающаяся для обеспечения надежного социального порядка в «обществе наблюдения».