

АНАЛИЗ УГОЛОВНОГО И УГОЛОВНО-ПРОЦЕССУАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА ГОСУДАРСТВ ЛАТИНСКОЙ АМЕРИКИ И КАРИБСКОГО БАССЕЙНА В СФЕРЕ ПРОТИВОДЕЙСТВИЯ НАСИЛИЮ В СЕТИ ИНТЕРНЕТ

Сравнение законодательства Российской Федерации и Республики Никарагуа представляет практический интерес в связи с развитием международного правоохранительного сотрудничества, подготовкой сотрудников компетентных органов иностранных государств и необходимостью понимания различий в подходах к регулированию цифровой преступности. Никарагуа использует модель специальных законов, концентрирующих значительную часть цифровой повестки в отдельных нормативных актах. Россия, напротив, применяет распределенную модель, при которой уголовно-правовые, процессуальные и регуляторные положения закреплены в различных кодексах и федеральных законах.

Наличие межведомственных и межгосударственных соглашений также подтверждает практическую значимость такого сопоставления. Для правоохранительного взаимодействия существенное значение имеет Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством внутренних дел Республики Никарагуа от 4 октября 2012 г., предусматривающее взаимодействие в предупреждении, выявлении, пресечении и раскрытии преступлений, включая преступления в сфере информационных технологий [14]. Для сферы ИКТ дополнительно значимо Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечения международной информационной безопасности от 19 июля 2021 г. [15].

Так правовое регулирование преступлений, совершаемых с использованием информационно-коммуникационных технологий (далее - ИКТ), а также противоправных действий с персональными данными в

Республике Никарагуа имеет комплексный характер. Общие составы преступлений закреплены в Уголовном кодексе Республики Никарагуа - Ley № 641, Código Penal [1]. Специальные составы деяний, совершаемых посредством ИКТ, информационных систем, компьютерных данных, цифровых идентификаторов, социальных сетей и мобильных приложений, сосредоточены преимущественно в Законе Республики Никарагуа № 1042 «Специальный закон о киберпреступлениях» (Ley Especial de Ciberdelitos) [2]. Общий режим обработки и защиты персональных данных установлен Законом № 787 «О защите персональных данных» (Ley de Proteccion de Datos Personales) [4].

Закон № 1042 закрепляет общее определение киберпреступлений и предусматривает составы, связанные с неправомерным доступом к информационным системам, компьютерным мошенничеством, хищением с использованием ИКТ, незаконным использованием и раскрытием персональных данных, подменой цифровой идентичности, распространением ложной или искаженной информации, угрозами и сексуальным домогательством через ИКТ. [2]. Реформа 2024 года, внесенная Ley № 1219, расширила сферу действия указанного закона, прямо включив социальные сети и мобильные приложения, а также закрепив применение закона к преступлениям, совершенным как на территории Никарагуа, так и за ее пределами [3].

Российское законодательство построено иначе. В Российской Федерации отсутствует единый закон о киберпреступлениях, сопоставимый по структуре с Ley № 1042. Уголовно-правовые запреты содержатся прежде всего в УК РФ, включая главу 28 «Преступления в сфере компьютерной информации», а также отдельные составы в иных главах, например ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации». Смежные понятия и режимы закреплены в федеральных законах об информации, персональных данных, связи и безопасности критической информационной инфраструктуры. Следовательно, ключевое различие состоит в степени концентрации регулирования:

никарагуанская более специализирована, российская - более распределена [8; 10; 11; 12].

В статье 3 Закона № 1042 киберпреступления определяются как действия или бездействие уголовного характера, совершаемые против физических и юридических лиц с использованием в качестве способа, средства или цели данных, информационных систем и ИКТ и направленные на причинение вреда личным, имущественным или информационным правовым благам потерпевшего. Такое определение позволяет рассматривать киберпреступность как самостоятельный объект законодательного регулирования [2].

В российском уголовном законодательстве общего легального определения понятия «киберпреступление» нет. УК РФ использует конструкцию конкретных составов преступлений. При этом в примечании к ст. 272 УК РФ раскрывается понятие компьютерной информации как сведений, сообщений, данных, представленных в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Понятия информационной системы, информационных технологий, информационно-телекоммуникационной сети, персональных данных, компьютерной атаки и компьютерного инцидента содержатся в специальном информационном законодательстве [8; 10; 11; 12].

Закон № 787 о защите персональных данных дополняет никарагуанскую систему: он определяет общий режим обработки данных в публичных и частных базах, права субъектов и обязанности лиц, осуществляющих обработку [4]. В России аналогичную функцию выполняет Федеральный закон № 152-ФЗ «О персональных данных», а уголовно-правовой блок дополнен, в частности, ст. 272.1 УК РФ, предусматривающей ответственность за незаконные действия с компьютерной информацией, содержащей персональные данные [8; 11].

В главе V УК Республики Никарагуа мошенничество сохраняет преимущественно традиционный характер и рассматривается как имущественное преступление. Вместе с тем цифровой способ совершения мошенничества прямо учитывается в ст. 229, предусматривающей

ответственность за получение несанкционированного перевода имущественного актива в ущерб третьему лицу путем манипулирования компьютерными записями, программами либо с использованием иного аналогичного приема [1].

Одновременно в Законе № 1042 предусмотрен самостоятельный состав компьютерного мошенничества - ст. 12 «*Fraude informatico*». Он охватывает получение имущественной выгоды для себя или третьего лица в ущерб другому лицу путем неправомерного использования ИКТ, манипулирования информационными системами, их компонентами, компьютерными данными либо содержащейся в них информацией. Смежными являются нормы о хищении с использованием ИКТ, манипуляциях со смарт-картами, подмене цифровой идентичности и неправомерном использовании персональных данных [2].

В российском уголовном законодательстве специальный состав мошенничества в сфере компьютерной информации закреплен непосредственно в УК РФ. Статья 159.6 УК РФ предусматривает ответственность за хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. При этом статья расположена в главе 21 УК РФ «Преступления против собственности», что отражает имущественный характер основного объекта посягательства [8].

Использование ИКТ в российском уголовном праве не образует универсального состава преступления. Оно может выступать способом совершения различных деяний, квалифицирующим признаком конкретных составов либо, в специально предусмотренных случаях, обстоятельством, отягчающим наказание. Поэтому российская система в большей степени исходит из оценки способа совершения деяния в рамках конкретной статьи Особенной части УК РФ [8].

В УК Республики Никарагуа предусмотрены общие составы преступлений против половой свободы и половой неприкосновенности, включая сексуальное домогательство, сексуальную эксплуатацию и порнографию. Уже в этих составах учитывается цифровая форма отдельных деяний: применительно к сексуальной эксплуатации и порнографии используется широкая формула распространения материалов любым способом, включая цифровой, аудиовизуальный, компьютерный, электронный или иной носитель [1].

Специальные цифровые формы таких деяний более предметно урегулированы в Законе № 1042. В нем выделены составы, связанные с использованием детей, подростков и лиц с инвалидностью в порнографии через ИКТ, предложениями лицам младше 16 лет для встреч сексуального или эротического характера либо производства порнографии, кибердомогательством и сексуальным домогательством через ИКТ. Распространение интимных изображений без согласия может охватываться нормой о неправомерном раскрытии данных или информации личного характера [2].

Никарагуанская модель дополнительно включает Закон № 779 «Всеобъемлющий закон о борьбе с насилием в отношении женщин» и Закон № 287 «Кодекс детства и подростков». Эти акты обеспечивают специальную институциональную рамку защиты женщин, детей и подростков, включая ювенальную уголовную юстицию и деятельность *Comisarias de la Mujer y la Ninez* - комиссариатов по делам женщин и детей. Наличие таких специализированных органов отличает никарагуанскую систему от российской [5; 6].

В Российской Федерации отсутствует единая категория «киберсексуальных преступлений» и нет федерального закона, полностью сопоставимого с Ley № 779. Охрана половой свободы, половой неприкосновенности, частной жизни и общественной нравственности в цифровой среде обеспечивается через совокупность норм УК РФ: ст. 133, 135,

137, 163, 242, 242.1, 242.2, 272.1 и иные составы. Современные формы, такие как sextortion, киберфлэшинг и сексуальные дипфейки, прямо не выделены как самостоятельные составы, но могут квалифицироваться через совокупность норм о понуждении, вымогательстве, нарушении неприкосновенности частной жизни, незаконном обороте порнографических материалов и персональных данных [8; 11; 13].

Уголовно-процессуальное законодательство Никарагуа содержит положения, направленные на сохранность и идентификацию объектов, имеющих доказательственное значение. Статьи 215 и 216 УПК Никарагуа предусматривают собирание, сохранение, идентификацию, инвентаризацию и безопасную охрану изъятых предметов, а также возможность получения копий или воспроизведений, если объекты могут исчезнуть, измениться или являются трудными для хранения. Для цифровых доказательств эти положения имеют значение при изъятии телефонов, компьютерной техники и иных носителей информации [7].

В российском уголовном процессе аналогичные задачи решаются через нормы о вещественных доказательствах, осмотре, изъятии, упаковке, хранении и процессуальном оформлении. Статья 81 УПК РФ определяет вещественные доказательства, ст. 82 - порядок их хранения, ст. 177 - порядок осмотра и изъятия предметов, а ст. 164.1 - особенности изъятия электронных носителей информации и копирования с них данных [9].

Существенное различие проявляется в вопросе доступа к содержимому электронных устройств. В Никарагуа такой доступ может рассматриваться как действие, потенциально затрагивающее конституционные права лица, включая неприкосновенность частной жизни, тайну сообщений и защиту персональных данных. Поэтому при необходимости извлечения и анализа информации Национальная полиция обращается за судебным разрешением, что следует из системного применения статей 227, 228, 230 и 246 УПК Никарагуа [7].

В Российской Федерации судебное разрешение требуется не на саму экспертизу изъятого электронного носителя, а на действия, прямо отнесенные

УПК РФ к судебному контролю. Общий перечень закреплён в ч. 2 ст. 29 УПК РФ, порядок получения разрешения - в ст. 165 УПК РФ. К таким действиям относятся, например, обыск и выемка в жилище, контроль и запись переговоров, наложение ареста на почтово-телеграфные отправления и получение информации о соединениях между абонентами и абонентскими устройствами. Российская модель тем самым разграничивает исследование уже изъятого объекта и получение охраняемой законом информации посредством специальных следственных действий [9].

Использование специальных знаний в Республике Никарагуа реализуется через проведение экспертных исследований (*peritaje*). Организационно такие исследования могут проводиться Институтом криминалистики и судебных наук Национальной полиции Республики Никарагуа (*Instituto de Criminalística y Ciencias Forenses*). В ведомственной форме заявки указывается вид исследования, обстоятельства дела, направляемые объекты, упаковка, маркировка, данные участников и вопросы эксперту. Компьютерная криминалистика выступает одним из направлений экспертной деятельности наряду с баллистическими, химическими, трасологическими, биологическими, документоскопическими и иными исследованиями [7].

В Российской Федерации использование специальных знаний осуществляется через процессуальные фигуры эксперта и специалиста. Эксперт даёт заключение как самостоятельный источник доказательств, а специалист содействует обнаружению, закреплению, изъятию и исследованию объектов, применению технических средств и постановке вопросов эксперту. Судебная экспертиза назначается постановлением следователя, дознавателя или суда по правилам ст. 195 УПК РФ, а заключение эксперта оформляется в соответствии со ст. 204 УПК РФ [9].

Следовательно, никарагуанская модель в большей степени демонстрирует ведомственно-организационный порядок направления объектов в экспертное подразделение Национальной полиции, тогда как российская модель строится вокруг процессуального решения о назначении судебной экспертизы, прав

участников, статуса эксперта и специалиста и процессуальной формы заключения [7; 9].

Таблица 1. Сравнительная характеристика отдельных элементов регулирования

Критерий	Республика Никарагуа	Российская Федерация
Общая модель	Специальные законы о киберпреступлениях, персональных данных, насилии в отношении женщин, детей и подростках.	Распределенная система: УК РФ, УПК РФ, законы об информации, персональных данных, связи и КИИ.
Понятие киберпреступления	Легальное определение закреплено в Законе №. 1042.	Единого определения нет; используются конкретные составы и понятие компьютерной информации.
Компьютерное мошенничество	Ст. 12 Закона №. 1042; цифровой способ также учтен в ст. 229 УК Никарагуа.	Ст. 159.6 УК РФ, расположенная в главе о преступлениях против собственности.
Персональные данные	Закон №. 787 и специальные составы Закона №. 1042.	152-ФЗ, ст. 272.1 УК РФ и смежные нормы УК РФ.
Цифровое насилие	Отдельные составы в Законе №. 1042, связь с Законом №. 779 и Кодексом детства и подростков.	Распределенная квалификация через нормы УК РФ о половой неприкосновенности, частной жизни, вымогательстве и порнографических материалах.
Судебный контроль	Более выраженная судебная санкционированность доступа к содержимому электронных устройств.	Судебное разрешение требуется для действий, прямо указанных в УПК РФ; экспертиза изъятого носителя назначается постановлением.
Экспертные исследования	Организационно встроены в систему Национальной полиции и Институт криминалистики и судебных наук.	Назначаются постановлением следователя, дознавателя или суда; разграничены эксперт и специалист.

Проведенное сопоставление показывает, что Республика Никарагуа и Российская Федерация используют различные законодательные модели противодействия преступлениям, совершаемым с использованием ИКТ. Никарагуанская модель характеризуется концентрацией специальных норм в отдельных законах и выраженной институциональной специализацией: Закон № 1042 объединяет значительный массив киберсоставов, Закон № 787 формирует режим персональных данных, Закон № 779 и Кодекс детства и подростков задают специальную рамку защиты женщин и несовершеннолетних, а Институт криминалистики и судебных наук Национальной полиции обеспечивает экспертно-криминалистическое сопровождение расследований [1; 2; 4; 5; 6; 7].

Российская модель имеет распределенный характер. Она не содержит единого легального определения киберпреступления и единого специального закона о киберпреступлениях, однако включает развитую систему конкретных составов УК РФ, процессуальных механизмов УПК РФ и специальных федеральных законов в сфере информации, персональных данных, связи и критической информационной инфраструктуры. Ее особенностью является более детальное разграничение материально-правовых, процессуальных и регуляторных режимов, а также четкое разграничение статусов эксперта и специалиста [8; 9; 10; 11; 12].

Практическое значение выявленных различий состоит в необходимости учитывать не только формальное совпадение отдельных составов, но и место соответствующей нормы в общей системе права. Для международного правоохранительного взаимодействия особенно важны различия в судебном санкционировании доступа к электронным устройствам, правовом режиме персональных данных, порядке экспертных исследований, защите несовершеннолетних и институциональной роли специализированных подразделений полиции. При подготовке учебных и методических материалов это позволяет точнее объяснять слушателям, почему сходные цифровые следы и преступные схемы в разных правовых системах получают различное процессуальное оформление и квалификационную оценку [14; 15].

ЛИТЕРАТУРА

1. Texto Consolidado, Ley N°. 641, Código Penal de la Republica de Nicaragua. Asamblea Nacional de Nicaragua.
2. Ley N°. 1042, Ley Especial de Ciberdelitos. Asamblea Nacional de Nicaragua.
3. Ley N°. 1219, Ley de Reformas y Adiciones a la Ley N°. 1042, Ley Especial de Ciberdelitos. Asamblea Nacional de Nicaragua. URL:
4. Ley N°. 787, Ley de Protección de Datos Personales. Asamblea Nacional de Nicaragua.

5. Texto Consolidado, Ley N°. 779, Ley Integral Contra la Violencia Hacia las Mujeres y de Reformas a la Ley N°. 641, Código Penal. Asamblea Nacional de Nicaragua.

6. Ley N°. 287, Código de la Niñez y la Adolescencia. Asamblea Nacional de Nicaragua.

7. Texto Consolidado, Ley N°. 406, Código Procesal Penal de la República de Nicaragua. Asamblea Nacional de Nicaragua.

8. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ.

9. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ.

10. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

11. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».

12. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

13. Федеральный закон от 24.06.1999 N 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних».

14. Соглашение о сотрудничестве между Министерством внутренних дел Российской Федерации и Министерством внутренних дел Республики Никарагуа от 4 октября 2012 г.

15. Соглашение между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечения международной информационной безопасности от 19 июля 2021 г. Официальный интернет-портал правовой информации.