Закон № 1042 эффективно дополняет нормы Уголовного кодекса (особенно статьи о насильственных действиях сексуального характера), поскольку устанавливает дополнительные квалифицирующие признаки: использование технологий, привлечение лиц с ограничениями, трансграничный характер распространения данных.

Кроме того, применение OSINT-инструментов (Epieos, Archive.is, WHOIS, 2ipdomaintools и др.) способствует идентификации злоумышленников даже при использовании фальсифицированных аккаунтов.

Анализ практики расследования преступлений, направленных против сексуальной свободы несовершеннолетних с использованием сети Интернет в Никарагуа, позволяет сделать вывод о целесообразности и своевременности принятия Закона № 1042. Этот нормативный акт стал эффективным инструментом защиты прав и свобод уязвимых категорий населения в условиях цифровизации. Опыт применения положений статьи 31 и 32 демонстрирует высокую значимость междисциплинарного подхода, сочетающего уголовно-правовые, криминалистические и технические аспекты расследования. Важно отметить, что международная кооперация и унификация стандартов хранения и анализа цифровых данных играют ключевую роль в повышении эффективности борьбы с киберпреступностью сексуального характера. Пример Джонатана Роча Перальты иллюстрирует, как системный подход и точное соблюдение процессуальных норм позволяют добиться справедливого наказания за преступления, совершенные в Интернете, и восстановить права потерпевших несовершеннолетних лиц.

Леонель Альберто Гарсиа Баес,
Эдди Маурисио Кастильо Мендьета,
Моисес Ноэль Пачеко Гарсиа,
Адонис Энрике Эскобар Вивас,
Хуан Карлос Эспиноза Пальма
Научное руководство при подготовке тезисов:
В.Ю. Жандров, кандидат юридических наук, доцент,
А.В. Токолов, кандидат юридических наук
(Московский университет МВД России имени В.Я. Кикотя)

Раскрытие мошенничества в сети Интернет

Развитие цифровых технологий коренным образом изменило способы социальной и экономической активности, включая взаимодействие между гражданами, государством и частным сектором. Вместе с тем эти достижения сопровождались ростом киберпреступности, среди которой все большую угрозу представляет собой мошенничество в сети Интернет. В Республике

Никарагуа, как и во многих других странах Латинской Америки, наблюдается увеличение числа дел, связанных с мошенничеством, совершаемым с использованием информационных технологий, включая подмену личности, фальсификацию документов, взлом электронных систем и неправомерное присвоение материальных ценностей посредством цифровых каналов.

К наиболее распространенным формам интернет-мошенничества относятся фишинг (получение конфиденциальных данных путем подделки легитимных сервисов), установка вредоносного ПО (malware), кража информации о банковских картах и онлайн-счетах, поддельные сайты интернет-торговли, а также незаконное присвоение личных данных (существующая как в форме кражи, так и в форме создания цифровых двойников). Каждая из этих форм предполагает использование Интернета как средства совершения преступления, в связи с чем возникает необходимость в правовой квалификации таких действий и выработке алгоритмов расследования, соответствующих как национальному законодательству, так и международным стандартам.

По состоянию на 2024 год количество пользователей социальных сетей в мире превысило 4,7 миллиарда человек, что составляет более половины населения планеты. В Никарагуа также наблюдается рост вовлеченности населения в цифровое пространство, особенно среди молодежи и представителей частного сектора. При этом 42% всего трафика электронной коммерции генерируется из социальных сетей, а 17% покупок осуществляется напрямую через цифровые платформы. Такой уровень цифровизации создает благоприятные условия не только для экономического роста, но и для действий злоумышленников.

Согласно статье 230 Уголовного кодекса Никарагуа (Ley № 641), мошенничество определяется как действие, направленное на введение в заблуждение другого лица с целью получения выгоды, что повлекло за собой ущерб как самому потерпевшему, так и третьим лицам. В случае если преступление совершается с использованием электронных средств, предусмотрены квалифицирующие обстоятельства, увеличивающие наказание. В частности, если деяние сопровождается злоупотреблением доверием, подменой личности, применением компьютерных технологий или затрагивает государственные ресурсы, преступление квалифицируется как отягчающее.

Ключевые элементы состава преступления по статье 230 включают наличие умысла на обман, использование методов, способных вызвать заблуждение, а также наступление имущественного ущерба. Закон предусматривает наказание в виде лишения свободы на срок от трех до шести лет и штраф от 300 до 500-дневных ставок, а при наличии отягчающих обстоятельств – более суровые меры.

Рассмотрим наглядный пример, раскрытый в Никарагуа в 2020 году. Гражданин по имени Шагер Омар Тобал Эскудеро, инженер по системам,

совершил серию действий, направленных на хищение строительных материалов у компании CEMEX Nicaragua через обман цифрового характера. Получив несанкционированный доступ к информационным системам мэрии Манагуа, он обнаружил контракт на поставку цемента между муниципалитетом и CEMEX. Используя полученные сведения, злоумышленник создал поддельный электронный адрес, идентичный адресу директора по закупкам мэрии, и отправил фальшивый заказ в компанию, указав ложные данные о транспортировке. В результате он получил 640 мешков цемента, используя вымышленных водителей и транспортные средства. Только после того, как мэрия обнаружила несоответствие в документации, было возбуждено уголовное дело.

Уголовное преследование в подобных случаях начинается с подачи заявления в органы полиции, прокуратуру или суд. Расследование проводит специализированное подразделение Национальной полиции – Dirección de Auxilio Judicial (DAJ), в том числе его отдел по борьбе с киберпреступностью. В процессе расследования могут быть применены такие меры, как изъятие электронных устройств, анализ сетевого трафика, блокировка подозрительных счетов, проведение компьютерной судебной экспертизы и получение цифровых доказательств в рамках международного сотрудничества. В соответствии со статьями 213 и 214 УПК Никарагуа (Ley № 406), органы следствия вправе ходатайствовать о применении превентивных мер и обеспечительных процедур.

В дополнение к статье 230 УК могут применяться статьи 240 (незаконное использование личности), 275 (фальсификация документов), а также положения о неправомерном доступе к электронным системам, пусть и не сформулированные в виде отдельной статьи, но допускаемые по аналогии правоприменительной практикой. Доказательная база в таких делах базируется на результатах цифровой экспертизы, свидетельских показаниях, анализе IP-логов, содержимом устройств и переписке в электронных почтовых ящиках.

Роль Министерства внутренних дел и Министерства юстиции в таких делах заключается в предоставлении информации по миграционному контролю, регистрации лиц и их судимости. Важно также отметить, что расследование цифрового мошенничества требует постоянного взаимодействия с частными технологическими компаниями и платформами (например, провайдерами электронной почты и хостинга), в том числе в рамках договоров о международном сотрудничестве в борьбе с киберпреступностью.

С учетом изложенного борьба с интернет-мошенничеством в Никарагуа предполагает комплексный подход, сочетающий нормативное регулирование, технические средства и институциональные механизмы. Выработка новых формул правовой квалификации, расширение полномочий следственных органов и создание единых протоколов межведомственного реагирования

представляются необходимыми шагами в условиях цифровой трансформации преступности.

Расследование случая с CEMEX и мэрией Манагуа подтвердило эффективность применения правовых норм статьи 230 УК в совокупности с доказательственной базой, собранной с помощью цифровой криминалистики. Обвинительный приговор, вынесенный в этом деле, стал важным прецедентом в практике применения традиционного уголовного законодательства к новым формам мошенничества, совершаемым в виртуальной среде.

В заключение следует подчеркнуть, что противодействие интернет–мошенничеству требует не только модернизации законодательства, но и повышения цифровой грамотности населения, внедрения механизмов раннего предупреждения и сотрудничества между государственными структурами и частным сектором. Интернет как пространство возможностей не должен становиться ареной безнаказанности для преступников — задача государства заключается в обеспечении правопорядка как в физическом, так и в цифровом измерении.

Татьяна Магали Кастельон Пикадо,
Ивания Патрисия Алеман Гонсалес,
Майела Элисабет Мартинес Мартинес,
Элиасер Давид Вивас Санчес-младший,
Мануэль Антонио Кальдера Гутьеррес
Научное руководство при подготовке тезисов:
В.Ю. Жандров, кандидат юридических наук, доцент,
А.В. Токолов, кандидат юридических наук
(Московский университет МВД России имени В.Я. Кикотя)

Противодействие распространению информации в социальных сетях, направленной на осуществление террористической деятельности

В современную эпоху цифровых технологий социальные сети стали не только средством общения, но и потенциальной платформой для организации, координации и пропаганды противоправных действий, включая террористическую деятельность. В условиях глобального информационного пространства особую актуальность приобретает проблема противодействия распространению контента, направленного на дестабилизацию общественно-политической обстановки и подрыв национальной безопасности. Республика Никарагуа, сталкиваясь с последствиями политической нестабильности, разработала эффективные механизмы реагирования на киберугрозы, включая