УДК 343.97

ПРЕСТУПНОСТЬ В СФЕРЕ ЦИФРОВОГО ОБОРОТА БИОМЕТРИЧЕСКИХ ДАННЫХ

Н. Ф. Бодров
президент международной общественной организации
«Союз криминалистов и криминологов»,
доцент кафедры судебных экспертиз
Московского государственного юридического университета имени О. Е. Кутафина (МГЮА),
кандидат юридических наук, доцент

Современные цифровые технологии трансформируют преступность, связанную с цифровым оборотом биометрических данных человека. В работе выявлены ключевые тенденции, включая рост открытости данных, утечки информации и доступность технологий синтеза и облачных сервисов. Отмечаются риски, связанные с распространением дипфейк–технологий.

Ключевые слова: преступность; биометрия; большие данные; цифровизация; дипфейки.

Биометрические данные человека в уголовно–правовых науках рассматриваются: 1) как предмет уголовно-правовой охраны, 2) как источники информации для раскрытия и расследования преступлений, 3) как объекты экспертного исследования.

Однако развитие цифровых технологий, больших данных и нейросетевых алгоритмов за недавний период существенно преобразовало как саму преступность в сфере оборота биометрических данных, так и методы борьбы с ней. Важной вехой в цифровизации стало развитие алгоритмов нейросетевой генерации на основе биометрических данных.

В законодательстве данные процессы нашли свое отражение в системе сбора статистической информации о состоянии преступности, например, в Приказе Генпрокуратуры России от 9 декабря 2022 г. № 746 «О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре». Так, в 2024 г. в Российской Федерации статистический учет средств, используемых при совершении преступлений, включает под кодом «049» «с использованием технологии дипфейк» – то есть тех преступлений, которые совершаются с применением нейросетевых алгоритмов фальсификации биометрической информации.

В уголовное законодательство России соответствующие изменения пока не вносились, хотя в рамках законопроектное деятельности был подготовлен проект федерального закона № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» (внесён 16 сентября 2024 г. депутатом Государственной Думы Я. Е. Ниловым, Сенатором Российской Федерации А. К. Пушковым).

В Республике Беларусь обсуждение технологий дипфейк на самом высоком уровне вовлечено в политический дискурс [1], является предметом научных исследований ная практика рассмотрения дел о применении подобных технологий уже формируется [3, с. 125] и демонстрирует определенные тенденции.

В первую очередь следует учесть тенденцию расширения доступа к технологиям, используемым при совершении преступлений в сфере оборота биометрических данных, которая приводит к вовлечению в совершение подобных преступлений субъектов, не обладающих углубленными знаниями и компетенциями в сфере компьютерных технологий.

Как с криминалистической, так и с криминологической и естественно с уголовно–правовой точки зрения меняется представление о личности и профессиональных навыках преступников. Высокотехнологичные орудия преступления становятся доступными более широкому кругу лиц. В основе этой тенденции лежит модель «программное обеспечение как услуга» (SaaS, от англ. Software as a Service) [4, с. 142]. Если раньше на основе выбранного преступником способа совершения преступления в сфере компьютерной информации можно было сделать вывод о его компетенциях и материально-технической обеспеченности, то теперь доступ к высокотехнологичным орудиям совершения преступления может получить практически любое лицо, обладающее доступом в интернет, т.к. все вычисления будут производиться в облачной инфраструктуре, а не на оборудовании пользователя. При этом и сам пользователь может не обладать навыками программирования или настройки аппаратно-программных комплексов. Более того, прослеживается тенденция того, что такие навыки с учетом развития сервисов и нейросетевых инструментов становятся вторичными. На смену специалистам по компьютерным технологиям в совершение преступлений вовлекаются, например, подростки, как в случае с распространением дипфейк-материалов в городе Альмендралехо [5, с. 238], где преступления совершала группа из 15 несовершеннолетних злоумышленников.

Далее следует констатировать, что критически важными для цифровой трансформации преступности в сфере оборота биометрических данных являются такие элементы номенклатуры облачных вычислений как: «Видеонаблюдение как услуга» (VSaaS, от англ. Video Surveilliance as a Service) [6, с. 198], «Инфраструктура как услуга» (IaaS, от англ. Infrastructure as a Service), «Платформа как услуга» (PaaS, от англ. Platform as a Service) [7, с. 188]. Подобного рода услуги и характер их оказания существенно влияют как на технологии розыска преступников, так и на характер цифровых следов, которые должны быть зафиксированы по такого рода делам.

Важной криминологически значимой предпосылкой увеличения доли преступлений в сфере цифрового оборота биометрических данных человека является то, что в открытом доступе в социальных сетях, мессенджерах и на других ресурсах накоплен и хранится значительный объем больших данных (разноракурсных изображений внешности, образцов голоса, материалов видеофиксации) массив которых достаточен для обучения нейросетевых алгоритмов, предоставляемых преступникам «как услуга». Дополнением к этому уже сейчас являются масштабные утечки персональной информации и биометрических данных, а также добровольная передача биометрических данных пользователями с использованием различных сервисов и приложений.

Логично предположить и то, что в корпоративной среде большие данные будут все более бесконтрольно использоваться для обучения нейросетей. Такую тенденцию можно проследить, например, в решении по делу Bartz v. Anthropic PBC, Case No. 3:24–cv–05417–WHA, Order of June 23, 2025 (N. D. Cal.), Федерального окружного суда Северного округа Калифорнии США. Суд признал, что использование законно приобретённых произведений для обучения ИИ является добросовестным даже при отсутствии согласия правообладателей.

Вероятно, что накопленные на информационных ресурсах биометрические данные в ближайшем будущем ждет аналогичная участь. А с учетом темпов и объемов утечек информации в корпоративной среде следует ожидать и роста преступности с использованием биометрических данных пользователей.

Еще одной тенденцией является усовершенствование технологий телефонного мошенничества. Если сейчас в инструментарии преступников имеются достаточно подробные персональные данные населения, то в обозримом будущем логично предположить трансформацию способов совершения подобного рода преступлений с использованием технологий синтеза звучащей речи (например, клонирования голоса и речи родственников и близких людей потерпевших) а также использование технологий подмены внешности с последующим использованием технологий видеосвязи.

Достаточно непростая ситуация сложилась с мерами по борьбе с современными телефонными мошенничествами. В связи с принятием Федерального закона от 1 апреля 2025 г. № 41–ФЗ «О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации», а также с учетом Федерального закона от 29 декабря 2022 г. № 572–ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» основной задачей обеспечения информационной безопасности общества станет предотвращение заполнения базы данных госинформсистемы «Антифрод» моделями голосов законопослушных граждан, так как именно на основе их открытых данных злоумышленники наиболее вероятно будут пользоваться сгенерированными голосами.

В данном случае российский опыт организационных мер по борьбе с кражей идентичности будет хоть и новаторским, но во многом полезным в том числе и для выработки аналогичного инструментария в Республике Беларусь.

Острой проблемой в судопроизводстве уже сейчас становится фальсификация цифровых доказательств. На основе открытых данных, массив которых достаточен для генерации, стороны предоставляют в уголовные и гражданские дела цифровые доказательства, содержание которых искажается или полностью имитируется с использованием нейросетевых алгоритмов генерации аудио-, видео- и текстовых материалов. Уже сейчас есть все основания полагать, что синтезированные диктофонные записи, записи камер видеонаблюдения и прочие доказательства, предоставляемые в цифровой форме, предоставляются в качестве доказательств по уголовным и гражданским делам. С развитием технологий их количество и качество будет только возрастать.

На сегодняшний день готовность правоохранительных органов к выявлению, расследованию преступлений, а также и технологическую обеспеченность профессионального судебно-экспертного сообщества к исследованию синтезированных материалов оценить достаточно сложно, так как методические рекомендации по наиболее востребованным направлениям соответствующей деятельности в настоящее время отсутствуют.

Указанные тенденции во многом уже сейчас предопределяют характер преступности в сфере цифрового оборота биометрических данных человека, в то же время как векторы ответных мер правоохранительной деятельности пока не так хорошо очерчены.

Библиографический список

1. Участие в Форуме медийного сообщества Беларуси в Могилеве [Электронный ресурс] // Офиц. интернет–портал Президента Респ. Беларусь [сайт]. – Минск, 2020. – 11 февр. – URL: https://president.gov.by/ru/events/ucastie–v–forume–medijnogo–soobsestva–belarusi–v–mogileve (дата обращения: 10.08.2025).

2. Казак, Т. В. Возможные перспективы генеративного искусственного интеллекта в Республике Беларусь /Т. В. Казак, А. Н. Василькова // Big Data и анализ высокого уровня : сб. науч. ст. XI междунар. науч.–практ. конф., Минск, 23–24 апр. 2025 г. / Белорус. гос. ун–т информатики и радиоэлектроники; редкол. : В. А. Богуш. – Минск, 2025. – С. 220–228.

3. Бодров, Н. Ф. Анализ судебной практики установления обстоятельств в случаях противоправного распространения генеративного контента, созданного с помощью технологий искусственного интеллекта / Н. Ф. Бодров, А. К. Лебедева // Юридические исследования. – 2024. – № 11. – С. 1–25.

4. Карпычев, В. Ю. Особенности правового регулирования оборота программного обеспечения, реализуемого на основе SaaS–технологий / В. Ю. Карпычев, М. В. Карпычев, Ю. П. Шальнова // Юридическая наука и практика: Вестн. Нижегород. Акад. МВД России. – 2017. – № 4 (40). – С. 141–146.

5. Badiola Coca, S. Pornographic Deepfakes and Minors: Policy Brief – The Almendralejo Case / S. Coca Badiola // Didactic and applied victimology: case analysis / G. Varona (ed.). – Murcia: Laborum, 2025. – P. 229–242.

6. Глебус, В. В. Особенности разработки стратегии позиционирования на рынке VSAAS / В. В. Глебус // Тенденции развития экономики и менеджмента : сб. науч. тр. по итогам междунар. науч.–практ. конф., Казань, 11 июня 2016 г. – Казань : Инновац. центр развития образования и науки, 2016. – Т. 3. – С. 198–200.

7. Павлуцких, М. В. Облачные сервисы IaaS, SaaS, PaaS – инфраструктура как услуга / М. В. Павлуцких, А. У. Есембекова, А. Ю. Анфалова // Глобальная трансформация и устойчивость экономики современной России : сб. ст. междунар. науч.–практ. конф., Сочи, 5-8 окт. 2022 г. / под ред. Х. А. Константиниди, В. В. Сорокожердева, Н. В. Агазаряна. – М. : АНО «НИИ истории, экономики и права», 2022. – С. 186–190.