УДК 343.98

Рождайкина Екатерина Игоревна
Южно-Уральский государственный университет
Юридический институт
Россия, Челябинск
rzhdekat@yandex.ru
Rozhdaykina Ekaterina
South Ural State University
Law Institute
Russia, Chelyabinsk

ПРОБЛЕМЫ ЗАЩИТЫ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация: на фоне развития информационных технологий биометрические персональные данные становятся наиболее уязвимыми и требуют защиты не только от посягательств злоумышленников, но и обеспечения их безопасности в ходе расследования преступлений. Статья посвящена исследованию нарушений конфиденциальности биометрических персональных данных при расследовании преступлений. Автором рассматриваются основные проблемы, связанные с исследованием биометрических данных, возникающие в правоприменительной практике при расследовании преступлений, предлагаются пути их решения.

Ключевые слова: биометрия, персональные данные, мошенничество, идентификационные базы, конфиденциальность, расследование преступлений.

PROBLEMS OF PROTECTION OF BIOMETRIC PERSONAL DATA WHEN INVESTIGATING CRIMES

Annotation: against the backdrop of the development of information technology, biometric personal data becomes the most vulnerable and requires protection not only

from attacks by attackers, but also to ensure their safety during the investigation of crimes. The article is devoted to the study of violations of the confidentiality of biometric personal data during the investigation of crimes. The author examines the main problems associated with the study of biometric data that arise in law enforcement practice during the investigation of crimes, and suggests ways to solve them.
Key words: biometrics**,** personal data, fraud, identification databases, confidentiality, investigation of crimes.

Персональные данные играют важную роль в жизни любого человека и от их сохранности зависит уровень безопасности жизни общества. В статье 2 Конституции РФ закреплено, что человек, его права и свободы являются высшей ценностью [1]. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства. Именно поэтому, государство стремится создать необходимые условия для развития безопасного оборота персональных данных.

За последние годы биометрия (уникальные физиологические или поведенческие характеристики для идентификации личности) стала широко используемой технологией в банковской сфере. Ее главное преимущество заключается в том, что она предоставляет надежный способ идентификации человека и защиты его финансовых средств.

Однако, с развитием технологий, преступники находят новые способы обхода системы биометрической идентификации посредством совершения преступных действий.

В последние годы наблюдается рост мошенничества с использованием биометрии в банковской сфере, а расследование таких преступлений становится приоритетным для правоохранительных органов и специалистов информационной безопасности.

Использование биометрии при расследовании преступлений включает в себя анализ и сопоставление уникальных физиологических и поведенческих характеристик человека с целью идентификации и сбора улик. Основными методами биометрии, используемыми в следственной деятельности, являются: папиллярные узоры рук, распознавание лица, распознавание голоса, распознавание сетчатки глаза, данные ДНК, анализ поведенческих реакций.

Одним из наиболее распространенных видов мошенничества с использованием биометрии является подделка биометрических данных и обман системы идентификации. Мошенники подделывают отпечатки пальцев, лица или другие биометрические характеристики, с целью получения доступа к чужому аккаунту или выполнения иных незаконных операций. Также применяются различные методы, как психологические, так и физические, чтобы заставить жертву предоставить свои биометрические данные самостоятельно и подтвердить «желаемые» операции [2].

Так, например, в 2021 году в Зеленограде было возбуждено уголовное дело по факту списания денежных средств с банковской карты с использованием верификации по голосу [3]. Для достижения цели мошенники попросили ответить утвердительно или отрицательно на вопрос: «Согласны ли Вы заблокировать счета карт, с которых были попытки списаний неизвестными?» После получения утвердительного ответа на заданный вопрос на банковский счет потерпевшего были перечислены денежные средства, после чего произошло их дальнейшее списание вместе с личными средствами.

Для оптимальной защиты биометрических данных и ускорения процесса расследования большое значение имеет не только реакция самого субъекта биометрии, но и оператора этих данных. Так, например стоит обратить внимание, что расследование мошенничества с использованием биометрии в банковской сфере начинается уже на этапе внутреннего расследования банковской организацией с момента фиксации обнаружения мошеннической активности. На данном этапе банк использует системы защиты от

мошенничества или антифрод-системы, адаптированные под требования банка, позволяющие обнаруживать аномальное поведение клиентов и реагировать на подозрительную активность, блокируя транзакции [4, с. 47]. То есть, если система замечает подозрительные попытки доступа или несоответствие биометрических данных, она может сигнализировать о возможном мошенничестве, после чего происходит анализ биометрических данных. В случае возникновения подозрений система должна анализировать биометрические данные, включая отпечатки пальцев, сетчатку глаза или сканирование лица, чтобы определить, является ли клиент настоящим или мошенником. Это может включать сравнение данных с уже существующей базой данных или проведение дополнительных проверок подлинности.

В случае подтверждения мошенничества с использованием биометрии, банковские организации должны сотрудничать с правоохранительными органами для установления преступников и пресечения дальнейших мошеннических действий. Сотрудничество выражается в предоставлении собранных данных соответствующими службами банка правоохранительным органам в процессе расследования.

С одной стороны, наличие идентификационных баз, применяемых при расследовании преступлений правоохранительными органами безусловно является неотъемлемым и эффективным способом расследования преступлений, однако с другой стороны возникает вопрос насколько безопасными такие системы являются для субъекта персональных данных и могут ли быть нарушены их права и интересы.

Стоит обратить внимание на то, что при применении биометрии при расследовании преступлений может возникнуть ряд следующих проблем:

Во-первых, наличие технических проблем. Для точного использования биометрических данных при расследовании, необходимо специальное техническое оборудование, которое сканирует отпечатки пальцев, проводит испытание с двухфакторной аутентификацией и прочее. Отсутствие

современных и качественных технологий может негативно сказаться на точности и эффективности использования биометрических данных при расследовании.

Во-вторых, недостаточная точность имеющихся идентификационных баз. Данная проблема вытекает из технической проблемы, так как технологии биометрии не всегда точны, как и человек может отличаться от своей биометрической модели.

Возможны ошибки при сопоставлении биометрических данных с реальными людьми. Это может привести к ошибочной идентификации и ложному обвинению. Так, например, из-за технической ошибки невиновное лицо может стать подозреваемым в совершении преступления с соответствующими для него негативными последствиями.

В-третьих, ограниченный доступ к данным. Для использования биометрических данных в расследовании, необходимо иметь доступ к большим объемам данных, которые могут находиться под защитой, зашифрованными или ограниченными политикой конфиденциальности банка, находиться в иных системах, что может привести к затруднению расследования.

В-четвертых, отсутствие специальных знаний у сотрудников правоохранительных органов в области использования биометрических данных и технологий. В большей степени биометрические системы идентификации пользователей – это знания в области финансов, банковского дела, статистических моделей, вычислительной техники и т.д. Поэтому при расследовании необходимо привлечь специалистов, компетентных в сетевых информационных технологиях, аппаратно-программных средствах; практических работников из банковской сферы и аудиторов [5, с. 20]. Знания специалистов, компетентных в сетевых информационных технологиях, аппаратно-программных средствах, позволяют отследить организацию процесса и особенности совершения таких преступных посягательств. Практические работники из банковской сферы, аудиторы, могут

проанализировать проведенные расчеты и дать им оценку, а также выявить противоправные схемы, к примеру отмывание денежных средств, полученных преступным путем.

В-пятых, необходимость соблюдения конфиденциальности и этики. Использование биометрических данных при расследовании может привести к нарушению конфиденциальности и этики. Поскольку сбор и использование биометрических данных без требуемого согласия субъекта персональных данных нарушает его права и угрожает частной жизни.

Как указывалось ранее, одной из причин использования биометрии при расследовании является ограниченность доступа к данным, так как имеющиеся идентификационные базы правоохранительных органов не содержат всех биометрических данных.

С декабря 2021 года Единая биометрическая система (далее ЕБС) официально приобрела статус государственной информационной системы. В 2023 году содержание этой системы значительно увеличено за счет организаций, ранее собиравших биометрию. Говоря о высокой степени защиты системы в виде цифрового кода акцент всегда делается на технические характеристики, однако не всегда учитывается человеческий фактор и защита теряет свой смысл при непосредственном похищении, копировании, изменении биометрических данных на стадии их получения банком или при занесении их в информационную базу [6, с. 194]. По мотивированному запросу правоохранительные органы вправе получать доступ к ЕБС и использовать полученные данные изображения лица и (или) данные голоса человека [7] для расследования.

Стоит отметить, что персональные данные, находящиеся в одном месте в большей степени подвержены опасности, так как в современном мире усовершенствуются не только способы защиты данных, но и способы кражи данных. Таким образом в случае получения злоумышленником доступа к ЕБС биометрия может быть подвержена копированию, изменению, удалению. В

последующем использование этих данных в преступных целях может нанести ущерб невиновным лицам. Отсутствие необходимой защиты данных может привести к предоставлению для расследования уже искаженных и недостоверных данных.

Так, например в случае утечки биометрии или неправомерного доступа к ЕБС гражданином С. была использована запись голоса гражданина Н. и с ее помощью было сообщено о готовящемся теракте сотрудникам полиции. Используя имеющиеся базы, было установлено, что голос действительно принадлежит гражданину Н. в отношение которого было возбуждено уголовное дело.

Несмотря на то, что биометрия индивидуальна и практически не может быть подделана, развитие технологий не стоит на месте и на практике удается неправомерно получать доступ к чужим аккаунтам с помощью биометрии. Ввиду того что биометрические данные становятся публичными и их можно найти в социальных сетях, преступник может создать маску на лицо с фотографией любого пользователя и таким образом расплачиваться в магазине от чужого имени [6, с. 197].

Подводя итог, хочется отметить, что в настоящее время отсутствуют установленные четкие методики расследования преступлений, совершаемых с использованием биометрических данных, также не имеется отдельного исследования в сфере использования биометрических технологий в раскрытии и расследовании преступлений [7, с. 151].

Для того чтобы обезопасить субъекта биометрических персональных данных при расследовании преступлений необходимо: во-первых, использование современного и качественного оборудования, способного поддерживать эффективную и многозадачную работу; во-вторых, создание высокого уровня систем защиты идентификационных баз с постоянным усовершенствованием уровня безопасности; в-третьих, повышение квалификации сотрудников правоохранительных органов в области

информационных технологий и разработка методик по выявлению, раскрытию и расследованию преступлений, связанных с биометрическими данными.

Список литературы:

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г.) // Российская газета, № 144, 04.07.2020.

2. Мошенники придумали, как воровать деньги со счетов с помощью биометрических данных [Электронный ресурс] // URL: https://www.bfm.ru/.

3. Окружная электронная газета Зеленоградского административного округа [Электронный ресурс] URL: https://www.zelao.ru.

4. Свинцицкий А.,Сердюк В. Основные векторы атак на банки // BIS Journal. 2017. №3(26). С. 46-47.

5. Жильцова Ю.В., Саванина И.Р. Обоснование применения комплексного подхода в судебной экспертизе на примере биометрической системы идентификации банковских пользователей // Бухгалтерский учет в бюджетных и некоммерческих организациях. 2021, № 14. С. 14 - 26.

6. Желудков М. А., Бетина А.Ю. Вопросы защищенности биометрических данных человека при реализации систем искусственного интеллекта и совершении преступлений // Актуальные проблемы уголовного права, криминологии, уголовного процесса и уголовно-исполнительного права: теория и практика : Материалы X Международной научно-практической конференции, Тамбов, 16–17 апреля 2021 года. – Тамбов: Издательский дом "Державинский", 2021. С. 193-198.

7. Постановление Правительства РФ от 28 декабря 2018 г. № 1703 «О предоставлении оператором единой биометрической системы и оператором регионального сегмента единой биометрической системы в Министерство внутренних дел Российской Федерации и Федеральную службу безопасности Российской Федерации сведений, содержащихся в единой биометрической

системе и региональном сегменте единой биометрической системы» // Собрание законодательства РФ, № 53 (часть II), 31.12.2018.

8. Гаужаева В. А., Лифанова Л. Г. Биометрическая идентификация в криминалистике // Аграрное и земельное право. 2023. № 3 (219). С. 151-154.