УДК 004.056.53

ПРОБЛЕМА ОБЕСПЕЧЕНИЯ ПРАВА НА ОХРАНУ ЧАСТНОЙ ЖИЗНИ ПРИ ОБРАБОТКЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

Камаева Дарина Евгеньевна, *студентка 2 курса института экономики и управления АПК, ФГБОУ ВО РГАУ−МСХА имени К. А. Тимирязева, e-mail: kamaeva.darina@mail.ru*
Тропина Дарья Владимировна, *к.ю.н., доцент кафедры экономической безопасности и права института экономики и управления АПК, ФГБОУ ВО РГАУ−МСХА имени К. А. Тимирязева, e-mail: tropina@rgau-msha.ru*

Аннотация. *В статье рассмотрено понятие биометрических данных, виды, способы защиты биометрических данных, правовое регулирование сбора, обработки и хранения биометрических данных в Российской Федерации.*
Ключевые слова: *персональные данные, биометрические данные, правовое регулирование, право на неприкосновенность частной жизни.*

Любые персональные данные, включая биометрические, хранятся и обрабатываются в национальных регистрационных системах, которые являются основным элементом информационной политики развитых государств.

Несмотря на это, в ряде стран была оспорена необходимость сбора данных из-за нарушений конституционного права на охрану частной жизни [1]. Так, например, в 1991 г. Конституционный суд Венгрии постановил, что закон, позволяющий создание многоразового личного идентификационного номера, прямо нарушает конституционное право на неприкосновенность частной жизни [5].

Неприкосновенность частной жизни заключается в реализации права индивида на защиту персональных данных от кражи и использования их в неправомерной деятельности, неоправданного вторжения в личную жизнь.

Биометрические данные − сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных [2].

Кроме понятия в этой же статье прописано о возможности сбора и хранения биометрических данных без согласия на это человека, если этого требуют международные договоры Российской Федерации и законы.

Исходя из определения понятия, биометрические данные существуют двух видов: физические и поведенческие. К физическим относятся: ДНК-

дактилоскопия, аутентификация по акустическим данным уха, распознавание по рисунку глазных вен, распознавание лиц, распознавание по рисунку вен на пальцах, распознавание по отпечатку пальца, распознавание по отпечатку и движению стопы, геометрия руки, распознавание по радужной оболочке глаза, движению губ, распознавание по запаху тела, распознавание по отпечатку ладони, распознавание по рисунку вен на ладони, распознавание по сетчатке глаза, отражение света от кожи, распознавание по термограмме. К поведенческим относятся: динамика нажатия клавиш, распознавание по подписи, распознавание говорящего по голосу, распознавание по походке.

Главной угрозой неправомерного использования биометрических данных является возможность несанкционированного доступа к ним.

Согласно 152-ФЗ персональные данные могут храниться не дольше, чем этого требуют цели их обработки, после чего они должны быть удалены или обезличены. Местом хранения биометрических данных может выступать информационная система, либо же вне информационных систем на материальных носителях информации. К материальным носителям информации могут относиться флэш-накопители, диски и т. д. Стоит отметить, что бумажные носители к ним не относятся [2].

К технологиям хранения при использовании материальных носителей информации (далее – МНИ) должны применяться определенные условия для сохранения права на неприкосновенность частной жизни. Требования для МНИ приведены в Постановлении Правительства от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Согласно этому документу, МНИ должны обеспечивать:

- невозможность несанкционированного доступа;
- идентификацию информационной системы, в которую была записана данная биометрия;
- доступ к данным для уполномоченных лиц;
- защиту от несанкционированного изменения, записи или дополнения.

Технологии хранения биометрии вне информационной системы должны обеспечивать:

- доступ к данным для уполномоченных лиц;
- применение электронной цифровой подписи или других технологий для обеспечения целостности и неизменности данных на МНИ;
- проверку наличия согласия субъекта на обработку биометрии [3].

В основном биометрические персональные данные применяются в банковской сфере. Для это в некоторых банках существует Единая биометрическая система (ЕБС). Это небольшой выделенный отдел в организации, в котором происходит сбор, обработка и хранение биометрии. Все данные из ЕБС передаются в Единую систему идентификации и аутентификации.

ЕБС необходимо защищать в соответствии с Приказом Минкомсвязи от

25.06.2018 № 321. В нем установлены правила обработки биометрических данных, размещения и обновления, кроме этого зафиксированы необходимые технические составляющие для получения биометрии. Биометрические образцы нельзя снимать подручными средствами, данный Приказ определяет характеристики для изображения лица и голоса субъекта персональных данных [4].

Существует обязательное условие, без которого невозможно правомерно взять биометрические данные – отсутствие регистрации физического лица в Единой системе идентификации и аутентификации. Если лицо там не зарегистрировано, то организация предлагает это сделать, при наличии заявления, прямо на месте.

Обновление биологических данных производится по заявлению физического лица, либо спустя 3 года после последнего снятия образцов.

Таким образом, биометрические данные – важная и неотъемлемая часть жизни современного человека. Способность оплачивать лицом проезд, или снять деньги с банковского счета без пин-кода безусловно делает повседневную жизнедеятельность проще, но в тоже время создает новые угрозы для каждого человека и подвергает опасности право на неприкосновенность частной жизни, несмотря на правовую защиту персональных данных.

Библиографический список

1. Конституция Российской Федерации, принятая на всенародном голосовании 12 декабря 1993 года, с изм. и допол. от 01 июля 2020 года // СПС Консультант плюс (дата обращения 16.11.2022г.).

2. Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных» // СПС Консультант плюс (дата обращения 16.11.2022 г.).

3. Постановление Правительства РФ от 06 июля 2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» // СПС Консультант плюс (дата обращения 16.11.2022г.).

4. Приказ Минкомсвязи России от 25 июня 2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления биометрических персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» (Зарегистрировано в Минюсте России 04.07.2018 № 51532) // СПС Консультант плюс (дата обращения 16.11.2022г.).

5. **Смирнова, Я. В.** Проблема обеспечения права на охрану частной жизни при обработке биометрических данных в Европейском союзе / Я. В. Смирнова. [Электронный ресурс]. – Режим доступа: URL: https://aprp.msal.ru/jour/article/view/3320/2019.