



КОНСТИТУЦИЈАЛЫҚ ЖӘНЕ ӘКІМШІЛІК ҚҰҚЫҚ / КОНСТИТУЦИОННОЕ И АДМИНИСТРАТИВНОЕ ПРАВО / CONSTITUTIONAL AND ADMINISTRATIVE LAW

УДК 342.7
МРНТИ 10.15.59

А.М. Амиров¹, Ш.Ш. Шаяхметов²

¹Академия правоохранительных органов при Генеральной прокуратуре Республики Казахстан,
г. Косшы, Республика Казахстан

²Судебная администрация Республики Казахстан, г. Астана, Республика Казахстан

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБРАБОТКИ БИОМЕТРИЧЕСКИХ ДАННЫХ

Аннотация. В статье рассматриваются законодательные особенности, нововведения и опыт отдельных государств, а также Республики Казахстан в области регулирования процессов сбора и обработки биометрических данных. При этом авторами сделан значительный упор на подход зарубежных государств, поскольку их опыт в сфере защиты данных, обеспечения конфиденциальности и недопущения необоснованного вмешательства в частную жизнь считается передовым в мире. Проводится сравнение зарубежного и отечественного законодательства. Кроме того, в статье затрагивается опыт использования биометрических данных правоохранительными органами в целях борьбы с преступностью. Также приводятся примеры внедрения и применения механизмов биометрической аутентификации. Целью данной работы является изучение передового зарубежного опыта защиты биометрических данных для определения целесообразности и возможности его имплементации в Республике Казахстан.

Ключевые слова: биометрическая аутентификация; биометрические данные; биометрическая идентификация; защита персональных данных; распознавание лица; цифровые технологии; искусственный интеллект; конфиденциальность.

А.М. Әміров¹, Ш.Ш. Шаяхметов²

¹Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясы,
Қосшы қ., Қазақстан Республикасы

²Қазақстан Республикасының Сот әкімшілігі, Астана қ., Қазақстан Республикасы

БИОМЕТРИЯЛЫҚ ДЕРЕКТЕРДІ ӨНДЕУДІ ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ МӘСЕЛЕЛЕРІ МЕН БОЛАШАҒЫ

Аннотация. Мақалада жекелеген мемлекеттердің, сондай-ақ Қазақстан Республикасының биометриялық деректерді жинау және өңдеу процестерін реттеу саласындағы заңнамалық ерекшеліктері, инновациялары мен тәжірибесі талқыланады. Бұл ретте авторлары шет мемлекеттердің көзқарасына айтарлықтай назар аударды, өйткені олардың деректерді қорғау, құпиялылықты қамтамасыз ету және жеке өмірге негізсіз араласуға жол бермеу саласындағы тәжірибесі әлемде озық болып саналады. Шетелдік және отандық заңнаманы салыстыру жүргізілді. Сонымен қатар, мақалада құқық қорғау органдарының қылмыспен күресу үшін биометриялық деректерді пайдалану тәжірибесі қарастырылған. Сондай-ақ биометриялық аутентификация механизмдерін енгізу және қолдану мысалдары келтірілген. Бұл жұмыстың мақсаты биометриялық деректерді қорғаудың озық шетелдік тәжірибесін оны Қазақстан Республикасында имплементациялаудың орындылығы мен мүмкіндігін айқындау үшін зерделеу болып табылады.

Түйінді сөздер: биометриялық аутентификация; биометриялық деректер; биометриялық сәйкестендіру; жеке деректерді қорғау; бетті тану; цифрлық технологиялар; жасанды интеллект; құпиялылық.



A.M. Amirov¹, Sh.Sh. Shayakhmetov²

¹The Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Kossy c., the Republic of Kazakhstan

²Judicial administration of the Republic of Kazakhstan, Astana c., the Republic of Kazakhstan

PROBLEMS AND PROSPECTS OF LEGAL REGULATION OF BIOMETRIC DATA PROCESSING

Abstract. The article discusses the legislative features, innovations and experience of individual countries, as well as the Republic of Kazakhstan in the field of regulating the collection and processing of biometric data. At the same time, the authors place considerable emphasis on the approach of foreign countries, since their experience in the field of data protection, ensuring confidentiality and preventing unjustified interference in private life is considered advanced in the world. A comparison of foreign and domestic legislation is carried out. In addition, the article also touches on the experience of using biometric data by law enforcement agencies in order to combat crime. Examples of the implementation and application of biometric authentication mechanisms are also provided. The purpose of this work is to study the best foreign experience in the protection of biometric data to determine the feasibility and possibility of its implementation in the Republic of Kazakhstan.

Keywords: biometric authentication; biometric data; biometric identification; personal data protection; facial recognition; digital technologies; artificial intelligence; privacy.

DOI: 10.52425/25187252_2024_34_8

Введение. По мнению исследователей, европейское законодательство заложило основы защиты персональных данных и является правовым ориентиром при построении национального законодательства многими государствами. Между тем, в первых важных международных документах по защите данных, а именно Конвенции «О защите физических лиц при автоматизированной обработке персональных данных», принятой Советом Европы в 1981 году¹, а также Директиве 95/46/ЕС «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», принятой Европейским Парламентом и Европейским Союзом в 1995 году², понятие биометрических данных отсутствовало.

В связи с ростом применения биометрических данных, расширением сферы применения данной технологии и влияния на защиту персональных данных, в 2000-х гг. в Европе начался процесс законодательного урегулирования вопроса сбора и применения биометрических данных. В 2007 году представлено определение,

согласно которому под биометрическими данными понимались «биологические свойства, физиологические характеристики, живые черты или повторяющиеся действия, являющиеся уникальными для конкретного индивида и поддающиеся измерению, даже если используемые на практике для их технического измерения закономерности включают определенную степень вероятности».

Официальное определение понятию «биометрические данные» дано в статье 4(14) Общего регламента защиты персональных данных (General Data Protection Regulation, GDPR), где указано, что «биометрические данные» – это персональные данные, полученные в результате специальной технической обработки, которые касаются физических, физиологических или поведенческих черт физического лица, а также позволяют произвести или подтверждают однозначную идентификацию этого физического лица, например, изображение лица или дактилоскопические данные». Следует отметить, что GDPR разделяет биометрические и генети-

¹ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [Electronic resource] – Access mode: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108> (Access data: 24.03.2024).

² О защите физических лиц при обработке персональных данных и о свободном обращении таких данных: директива Европейского парламента и Совета Европейского Союза от 24 окт. 1995 г. № 95/46/ЕС [Электронный ресурс] – Режим доступа: https://online.zakon.kz/Document/?doc_id=31067635 (дата обращения: 04.04.2024).



ческие данные, относя к генетическим «персональные данные, относящиеся к наследственным или приобретенным генетическим характеристикам физического лица, которые раскрывают уникальную информацию о физиологии или здоровье человека, и которые являются результатом, в частности, анализа биологического образца данного физического лица» (ст. 4(13) GDPR)³.

В дальнейшем понятие «биометрические данные», а также требования к сбору и обработке такого вида персональных данных включены в законодательство многих государств. При этом имеет место, как точное дублирование GDPR, так и другие подходы [1].

Материалы и методы. В процессе данного исследования применялся метод анализа и сравнения зарубежного и отечественного законодательства, научных трудов ученых в сфере защиты персональных и биометрических данных.

Результаты/обсуждение. Вопрос сбора и обработки биометрических данных изучался многими иностранными исследователями, которые по итогу отмечают важность вопроса ввиду того, что процедура биометрической идентификации активно входит в повседневную жизнь населения, что требует надлежащего законодательного урегулирования.

По мнению Г. Сингх, Г. Бхардвадж, В. Сингх и В. Гарг, биометрические системы имеют преимущества над традиционными средствами идентификации личности, в связи с чем биометрические персональные данные становятся популярным средством аутентификации, но их массовый сбор и расширение применения представляют значительные риски для безопасности персональных данных [2].

А. Де Кейзер и другие, изучив возможности и проблемы использования биометрии в бизнесе, отмечают, что биометрические системы широко представлены в различных отраслях бизнеса и в ближайшей перспективе их применение в сфере бизнеса и маркетинга

будет расширяться, что влечет риски доступа к ранее недоступным персональным данным [3].

А. Иоанну, И. Тусядия и Я. Лу приводят примеры внедрения крупными авиационными и морскими перевозчиками пассажиров биометрических решений, позволивших значительно сократить сроки посадки большого количества пассажиров на самолеты или круизные лайнеры [4].

М. Смит и С. Миллер утверждают, что во взаимодействии с искусственным интеллектом биометрическое распознавание имеет значительный потенциал для раскрытия преступлений, но ввиду наличия рисков нарушения конфиденциальности требуется надлежащее законодательное урегулирование этого процесса. Имеют место этические противоречия между сбором биометрической информации для правоохранительных органов, национальной безопасности и предоставления государственных услуг, а также правом на неприкосновенность частной жизни. Для внедрения таких систем важным является наличие механизма защиты от злоупотреблений. Граждане должны быть информированы о биометрических процедурах и участвовать в них лишь с согласия [5].

В Казахстане согласно пункту 1 статьи 1 Закона «О персональных данных и их защите» под биометрическими данными понимаются персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность⁴. При этом законодательство не раскрывает, что понимается под физиологическими и биологическими особенностями субъекта персональных данных.

Законом «О дактилоскопической и геномной регистрации» закреплены два вида биометрических данных: геномная информация и дактилоскопическая информация. Геномная

³ Общий регламент защиты персональных данных (GDPR) Европейского союза [Электронный ресурс] – Режим доступа: <https://gdpr-text.com/ru/> (дата обращения: 18.09.2024).

⁴ О персональных данных и их защите: закон Республики Казахстан от 21 мая 2013 г. № 94-V [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm> (дата обращения: 18.10.2024).



информация содержит сведения о дезоксирибонуклеиновой кислоте (далее – ДНК), а дактилоскопическая об особенностях строения папиллярных узоров пальцев и (или) ладоней рук⁵.

В отличие от GDPR, законодательство Казахстана не разделяет биометрические и генетические персональные данные, напротив генетическая информация является видом биометрических данных. К сходствам можно отнести, что в определении и других нормах не перечислены возможные виды биометрических данных.

Следует отметить, что помимо вышеуказанных законов другие нормативные правовые акты Казахстана прямо не относят какие-либо персональные данные к биометрическим, но из их содержания следует, что биометрическими данными в Казахстане являются не только ДНК и папиллярные узоры. Например, Министерство внутренних дел в «Перечне персональных данных, необходимых и достаточных для выполнения осуществляемых задач» к персональным данным относит сведения, качественно и количественно характеризующие физиологические и биологические особенности человека и, на основе которых можно установить его личность: дактилоскопические; фотоизображение и видеозапись; голос и речь; ДНК; запах; группа крови и пр.⁶

Также в последние годы в законодательстве Казахстана все чаще появляются нормы о биометрической идентификации, которая осуществляется с помощью биометрических данных. К примеру, 20 августа 2024 года введен в действие пункт 5-5 статьи 34 Закона «О банках и банковской деятельности в Республике Казахстан», который обязывает

банки проводить биометрическую идентификацию для заключения договора банковского займа посредством Интернета⁷. Аналогичные требования введены в Закон «О микрофинансовой деятельности»⁸.

16 августа 2024 года приняты «Правила проведения биометрической идентификации банками, организациями, осуществляющими отдельные виды банковских услуг, и микрофинансовыми организациями», из которых следует, что биометрическая идентификация будет проводиться по изображению лица путем сличения текущего и эталонного изображения идентифицируемого лица⁹. «Правила и срок реализации пилотного проекта по использованию средств биометрической идентификации в информационной системе электронных счетов-фактур» предполагают, что биометрическая идентификация проводится по цифровой фотографии¹⁰.

Требования о биометрической идентификации включены и во многие другие нормативные правовые акты, в т.ч. относительно оказания социальных, государственных, финансовых услуг и других правоотношений.

Таким образом, законодатель допускает биометрическую идентификацию посредством разных видов персональных данных, но не относит их к биометрическим данным, хотя из содержания правовых актов и фактического предназначения в процедуре идентификации личности они являются именно биометрическими данными.

Следует отметить, что «Соглашение о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии, и использовании в государствах-

⁵ О дактилоскопической и геномной регистрации: закон Республики Казахстан от 30 дек. 2016 г. № 40-VI ЗРК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1600000040> (дата обращения: 14.10.2024).

⁶ Об утверждении перечня персональных данных, необходимого и достаточного для выполнения осуществляемых задач: приказ Министра внутренних дел Республики Казахстан от 12 авг. 2013 г. № 493 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/V1300008649> (дата обращения: 07.04.2024).

⁷ О банках и банковской деятельности в Республике Казахстан: закон Республики Казахстан от 31 авг. 1995 г. № 2444 [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/Z950002444_ (дата обращения: 24.10.2024).

⁸ О микрофинансовой деятельности: закон Республики Казахстан от 26 нояб. 2012 г. № 56-V [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z1200000056> (дата обращения: 24.10.2024).

⁹ Об утверждении Правил проведения биометрической идентификации банками, организациями, осуществляющими отдельные виды банковских услуг, и микрофинансовыми организациями: постановление Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 16 авг. 2024 г. № 56 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/V2400034950> (дата обращения: 20.10.2024).

¹⁰ Об утверждении Правил и срока реализации пилотного проекта по использованию средств биометрической идентификации в информационной системе электронных счетов-фактур: приказ и.о. Заместителя Премьер-Министра – и.о. Министра финансов Республики Казахстан от 27 марта 2023 г. № 294 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/V2300032132> (дата обращения: 20.10.2024).



участниках СНГ» к биометрическим данным относит цифровую фотографию, отпечатки пальцев, изображение радужной оболочки глаз и другие биометрические персональные данные¹¹.

При таких обстоятельствах неясным являются причины ненадлежащего законодательного урегулирования видов биометрических данных, порядка их сбора и обработки. Безусловно, внедрение биометрической идентификации во многих сферах в Казахстане в целом направлено на благие цели, однако отсутствие четких требований к сбору, хранению и применению многих видов биометрических сведений в будущем может вызвать существенные проблемы, особенно учитывая распространение в настоящее время дипфейк-технологий.

К примеру, банки второго уровня, которые начинают сбор биометрических данных клиентов, находятся в зоне риска. В 2021 году Центром анализа и расследования кибератак (ЦАРКА) выявлены уязвимости к атакам и утечке данных веб-ресурсов многих банков второго уровня Республики Казахстан (далее – РК)¹². 15 октября 2024 года Председатель Комитета информационной безопасности Министерства цифрового развития и аэрокосмической промышленности Р. Абдикаликов сообщил о наличии фактов утечек персональных данных клиентов из банков второго уровня¹³.

Имеющиеся проблемы в сфере применения биометрической аутентификации планировалось решить при реализации Программы создания Национальной платформы цифровой биометрической идентификации на 2022-2024 гг., но дальше обсуждения проекта она не зашла¹⁴.

В научной литературе к биометрическим персональным данным помимо фотографии, ДНК и папиллярных узоров также относят

радужную оболочку глаз, рост, вес, видеозапись лица, рисунок вен ладони.

По сведениям Г.С. Кодашевой на начало 2019 года в мире чаще всего применялись биометрические системы, основанные на распознавании отпечатков пальцев, рисунков вен, голоса и геометрия ладони, менее активно применялись технологии распознавания изображения лица, радужной оболочки глаза, поведенческой биометрии, ушных раковин и сигналов мозга [6].

Изучение информации из открытых источников показывает, что в жизни граждан Казахстана достаточно активно используются сервисы с применением технологий сбора и использования различных биометрических данных. При этом для идентификации личности используются не только фотографии и изображения человека, но и другие виды биометрических данных. Например, казахстанский стартап-проект «Alaqa» на протяжении нескольких лет внедряет в стране технологию использования рисунка вен ладони человека для входа в помещения и для оплаты услуг. По сведениям разработчиков, в системе зарегистрировались уже почти 100 тысяч человек.

Биометрические данные все чаще применяются и в деятельности правоохранительных органов

К примеру, К.О. Карабеков сообщает, что в Казахстане проводится целенаправленная работа по пресечению звонков с подменных номеров, используемых мошенниками. Министерством внутренних дел реализуется проект «Киберпол», что позволило пресечь более 43 миллионов таких звонков [7]. Также решение данной проблемы предполагается путем внесения в «Правила оказания услуг связи» требований об оказании услуг связи на основании договора между оператором и абонентом, подтвердившим свою личность биометрическими данными. Проект

¹¹ Об утверждении Соглашения о сотрудничестве в создании государственных информационных систем паспортно-визовых документов нового поколения и дальнейшем их развитии, и использовании в государствах-участниках СНГ: постановление Правительства Республики Казахстан от 30 марта 2009 г. № 430 [Электронный ресурс] – Режим доступа: https://adilet.zan.kz/rus/docs/P090000430_ (дата обращения: 12.09.2024).

¹² Результаты анализа защищенности веб-ресурсов банков второго уровня Республики Казахстан 2021. – 23 с. [Электронный ресурс] – Режим доступа: <https://cert.kz/files/reports/kz-banks-security-report-webtotem-2021.pdf> (дата обращения: 23.10.2024).

¹³ МЦРИАП: Сотрудники банков продавали личные данные казахстанцев [Электронный ресурс] – Режим доступа: <https://www.zakon.kz/obshchestvo/6452522-mtsriap-sotrudniki-bankov-prodavali-lichnye-dannye-kazakhstantsev.html> (дата обращения: 23.10.2024).

¹⁴ Об утверждении Программы создания Национальной платформы цифровой биометрической идентификации на 2022-2024 годы: проект постановления Правительства Республики Казахстан [Электронный ресурс] – Режим доступа: <https://legalacts.egov.kz/npa/view?id=14023459> (дата обращения: 09.09.2024).



изменений на стадии обсуждения¹⁵.

Органами прокуратуры в работе также активно применяются современные технологии, в т.ч. возможности биометрической идентификации.

6 августа 2024 года Генеральный Прокурор РК Б.Н. Асыллов через социальные сети и СМИ сообщил, что органами прокуратуры внедрена информационная система по автоматическому распознаванию скрывающихся преступников, должников и пропавших без вести, которая в двух городах страны подключена к видеокамерам наблюдения и позволила выявить 53 лица, находившихся в розыске¹⁶.

О.И. Лукьянчиков считает, что «современные методы распознавания лиц, представленные различными обученными моделями, демонстрируют высокую точность в условиях воздействия внешних факторов, обеспечивая в то же время сравнительно высокую производительность» [8].

С.А. Гречаный отмечает, что «правильно подобранная и установленная система будет работать с высокой точностью и сможет значительно помочь с обеспечением безопасности на любом объекте, выполняя работу, недоступную человеку. Как мы понимаем, человек не может, например, рассмотреть в толпе сразу десятки, а то и сотни лиц и быстро сравнить их с имеющимися у него тысячами ориентировок. Системы распознавания лиц, как и интеллектуальные системы видеонаблюдения в целом, непрерывно развиваются и, вместе с этим, становятся все более доступными» [9].

Д. Утеген и Б.Ж. Рахметов отмечают, что Европейский орган по надзору за защитой данных и Совет Европы выступали за запрет использования искусственного интеллекта для автоматического определения лиц в общественных местах, после чего такие положения были включены в Закон ЕС «Об

искусственном интеллекте». Между тем, данные ограничения касаются частных компаний, но не распространяются на правоохранительные органы [10].

Также Генеральной прокуратурой в 2024 году внесены изменения в «Правила формирования, доступа, использования, хранения, защиты и уничтожения сведений из системы информационного обмена правоохранительных, специальных государственных и иных органов», согласно которым теперь для входа в систему необходимо прохождение многофакторной аутентификации, включая проверку биометрии пользователя (отпечатков пальцев либо Face ID), либо подтверждение личности через SMS-код, что направлено на решение имевшихся ранее проблем по недостаточно эффективному контролю доступа к системе¹⁷.

Кроме того, на основании акта надзора Генеральной прокуратуры в качестве пилотного проекта в 37 медицинских объектах города Астана внедрен цифровой механизм подтверждения посещения медицинского специалиста, а с 2025 года такой опыт поэтапно будет внедряться по всей стране. Данный механизм предусматривает биометрическую идентификацию пациентов при посещении медицинских учреждений, что делает невозможным фальсификацию отчетов об оказанных медицинских услугах, а также предотвращает нецелевое расходование бюджетных средств. Внедрение технологии снизило статистические показатели оказанных медицинских услуг на 24,5%¹⁸.

В.В. Яцуценко полагает, что «основная цель внедрения цифровых технологий в деятельность органов прокуратуры заключается в достижении более эффективных результатов в поддержании законности в стране, доступности населению и прозрачности ее работы» [11]. Э. Киндт считает, что порядок

¹⁵ О внесении изменений в приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171 «Об утверждении правил оказания услуг связи»: проект приказа [Электронный ресурс] – Режим доступа: <https://legalacts.egov.kz/npa/view?id=15183499> (дата обращения: 22.10.2024).

¹⁶ В Алматы и Атырау внедрили «умные» камеры с ИИ [Электронный ресурс] – Режим доступа: <https://digitalbusiness.kz/2024-08-06/v-almati-i-atirau-vnedrili-umnie-kameri-s-ii/> (дата обращения: 01.09.2024).

¹⁷ Об утверждении Правил формирования, доступа, использования, хранения, защиты и уничтожения сведений из системы информационного обмена правоохранительных, специальных государственных и иных органов: приказ Генерального Прокурора Республики Казахстан от 13 янв. 2023 г. № 21 [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/V2300031702> (дата обращения: 15.10.2024).

¹⁸ Из материалов Генеральной прокуратуры Республики Казахстан по результатам проверки в сфере вакцинации и лекарственного обеспечения населения.



сбора и обработки биометрических данных, в т.ч. правоохранительными органами должен быть надлежащим образом урегулирован законодательно и содержать четкие указания относительно случаев недопустимости биометрической идентификации. Целесообразно вводить запреты или моратории на сбор отдельных видов биометрических данных за исключением крайней необходимости [12].

Следует отметить, что GDPR и зарубежное законодательство относят к биометрическим персональным данным не только физические и физиологические, но и поведенческие особенности физического лица, которые позволяют произвести или подтверждают однозначную идентификацию этого физического лица.

В иностранной научной литературе значительное внимание уделяется изучению поведенческих биометрических данных, поскольку сбор такой информации увеличивается, а некоторые из них собираются постоянно.

И.М. Альсаади изучены 4 наиболее используемые поведенческие биометрические системы: распознавание голоса, распознавание походки, распознавание подписи и динамика нажатия клавиш. Плюсом этих методов биометрической идентификации является их недороговизна, а также достаточно высокий уровень точности аутентификации. При этом каждая из систем имеет и свои минусы [13].

И. Стилиос и другие указывают, что мобильные устройства становятся все более технологичными, встроенные в них датчики уже сейчас позволяют собирать множество сведений о пользователе, осуществляя поведенческую биометрическую аутентификацию, в т.ч. сведения о голосе, походке, динамике нажатия клавиш, взмахах рук и многие другие данные [14].

Ф.В. Грушин отмечает, что в российском законодательстве поведенческие особенности не выделены как отдельная категория данных, но «исследования и внедрение в практику технологий идентификации исключительно по поведенческим характеристикам (таким как голос, подпись,

шаблоны ввода, походка, положение тела в пространстве и др.), дают основания полагать, что выделение данной категории в законодательном отражении возможно в ближайшем будущем» [15].

Полагаем, что в Казахстане в ближайшее время также возникнет необходимость законодательного урегулирования порядка сбора такой информации, поскольку уже сейчас осуществляется сбор сведений о поведенческих особенностях лиц.

В 2023 году принят Закон «Об онлайн-платформах и онлайн-рекламе», которым введены такие понятия, как профайлинг, под которым понимаются действия онлайн-платформ по определению предпочтений и (или) интересов пользователей и таргетированная онлайн-реклама, т.е. реклама, направляемая целевым группам на основании профайлинга¹⁹. Иными словами, онлайн-платформам дано право сбора информации о поведенческих особенностях человека.

Без надлежащего контроля за данным вопросом не исключены факты нарушения прав граждан. К примеру, В.И. Солдатова описывает имевший место в Российской Федерации случай предоставления оператором связи третьему лицу сведений об абонентах, их IP-адресах, предпочтениях и запросах в сети Интернет, что является нарушением их прав на защиту персональных данных [16].

В то же время полное блокирование сбора сведений о поведенческих особенностях человека нецелесообразно. Более того, применение таких сведений имеет существенные перспективы для использования в борьбе с преступностью. Внедрение сведений об особенностях походки, жестикуляции и других подобных данных, безусловно, способствовало бы повышению эффективности системы автоматического распознавания, а сбор образцов голоса преступников мог бы помочь в борьбе с интернет-мошенничеством.

Оптимальным решением могло бы стать совершенствование правовых норм

¹⁹ Об онлайн-платформах и онлайн-рекламе: закон Республики Казахстан от 10 июля 2023 г. № 18-VIII ЗПК [Электронный ресурс] – Режим доступа: <https://adilet.zan.kz/rus/docs/Z2300000018> (дата обращения: 01.10.2024).



относительно биометрических данных в рамках разрабатываемого Цифрового кодекса РК, принятие которого предполагает утрату силы Закона «О персональных данных и их защите».

Закключение. 1. По сравнению с казахстанским законодательство зарубежных государств в части регулирования сбора и обработки биометрических данных является более полным, проработанным и урегулированным. Генетическая информация в Казахстане относится к биометрическим данным, а в зарубежных странах к отдельному виду персональных данных – генетическим данным.

2. Несовершенство казахстанского законодательства в части регулирования сбора и обработки биометрических данных в определенной степени является сдерживающим фактором эффективной защиты персональных данных, в т.ч. работы государственных органов и прокурорского надзора в этой сфере.

3. Необходима доработка понятия «биометрические данные», определение и закрепление их видов, в т.ч. исходя из внедряемых в различных сферах общественных отношений и используемых гражданами средств биометрической идентификации, определение уровня конфиденциальности новых видов биометрических данных, порядка обработки и использования такой информации.

4. Требуется расширение применения понятия «биометрические данные», охватывая им сведения не только о физиологических и биологических, но и о поведенческих особенностях человека, поскольку такая информация не только представляет повышенный интерес частных компаний, но и уже собирается, а также может быть полезна в борьбе с преступностью.

5. Совершенствование правовой базы института биометрических данных в РК целесообразно в рамках разрабатываемого цифрового законодательства.

Список использованной литературы:

1. Смирнова, Я.В. Особенности содержания понятия «биометрические данные» в праве Европейского Союза / Я.В. Смирнова // Вестник Университета имени О. Е. Кутафина. – 2021. – № 7 (83). – С. 160-167.
2. Singh, G. Biometric Identification System: Security and Privacy Concern / G. Singh, G. Bhardwaj, S.V. Singh, V. Garg // Artificial Intelligence for a Sustainable Industry 4.0., 2021. – 323 p.
3. De Keyser, A. Opportunities and challenges of using biometrics for business: Developing a research agenda / A. De Keyser, et al. // Journal of Business Research. – 2021. – № 136. – Pp. 52-62.
4. Ioannou, A. Privacy concerns and disclosure of biometric and behavioral data for travel [Electronic resource] / A. Ioannou, I. Tussyadiah, Y. Lu // International Journal of Information Management. – 2020. – № 54. – Access mode: <https://www.sciencedirect.com/science/article/abs/pii/S0268401219317311> (Access data: 15.04.2024).
5. Smith, M. The ethical application of biometric facial recognition technology / M. Smith, S. Miller // AI & Soc. – 2022. – № 37. – Pp. 167-175.
6. Кодашева, Г.С. Удаленная биометрическая идентификация в банковской сфере Казахстана как часть цифровой инфраструктуры // Финансовые аспекты третьей модернизации экономики Казахстана: сб. материалов междунар. научн.-практич. конф. – 2021. – С. 405-413.
7. Карабеков, К.О. Состояние и тенденции киберпреступности в Российской Федерации и Республике Казахстан / К.О. Карабеков // Научный вестник Омской академии МВД России. – 2024. – № 30 (2 (93)). – С. 106-112.
8. Лукьянчиков, А.И. Принцип работы систем распознавания лиц и особенности их применения при обработке видеопотока в реальном времени / А.И. Лукьянчиков и др. // Информатика и вычислительная техника и управление. Серия: Естественные и технические науки. – 2023. – № 5. – С. 76-83.
9. Гречаный, С.А. Распознавание лиц в современных системах видеонаблюдения. На примере оборудования ТМ / С.А. Гречаный, Н.Ю. Федина, М.В. Храмыков // Охрана, безопасность,



связь. – 2020. – № 5-1. – С. 63-68.

10. Утеген, Д. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования / Д. Утеген, Б.Ж. Рахметов // *Journal of Digital Technologies and Law*. – 2023. – № 1 (3). – С. 825-844.

11. Яцуценко, В.В. Проблемы и перспективы внедрения цифровых технологий в деятельность органов прокуратуры / В.В. Яцуценко // *Актуальные проблемы российского права*. – 2021. – № 11 (132). – С. 187-193.

12. Kindt, E. A first attempt at regulating biometric data in the European Union // *Regulating biometrics: Global approaches and urgent questions*. – 2020. – Pp. 62-69.

13. Alsaadi, I.M. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review / I.M. Alsaadi // *International journal of scientific & technology research*. – 2021. – № 10. – Pp. 15-21.

14. Stylios, I., Behavioral biometrics & continuous user authentication on mobile devices: A survey / I. Stylios, et al. // *Information Fusion*. – 2021. – № 66. – Pp. 76-99.

15. Грушин, Ф.В. Фотоизображение и описание примет осужденных к лишению свободы как вид персональных данных, подлежащих обработке в уголовно-исполнительной системе России / Ф.В. Грушин, А.Ю. Сивцова // *Вестник Самарского юридического института*. – 2022. – № 1 (47). – С. 45-51.

16. Солдатова, В.И. Защита персональных данных в условиях применения цифровых технологий / В.И. Солдатова // *Lex russica*. – 2020. – № 2 (159). – С. 33-43.

References:

1. Smirnova, Ja.V. Osobennosti soderzhaniya ponjatija «biometricheskie dannye» v prave Evropejskogo Sojuza / Ja.V. Smirnova // *Vestnik Universiteta imeni O. E. Kutafina*. – 2021. – № 7 (83). – S. 160-167.

2. Singh, G. Biometric Identification System: Security and Privacy Concern / G. Singh, G. Bhardwaj, S.V. Singh, V. Garg // *Artificial Intelligence for a Sustainable Industry 4.0.*, 2021. – 323 p.

3. De Keyser, A. Opportunities and challenges of using biometrics for business: Developing a research agenda / A. De Keyser, et al. // *Journal of Business Research*. – 2021. – № 136. – Pp. 52-62.

4. Ioannou, A. Privacy concerns and disclosure of biometric and behavioral data for travel [Electronic resource] / A. Ioannou, I. Tussyadiah, Y. Lu // *International Journal of Information Management*. – 2020. – № 54. – Access mode: <https://www.sciencedirect.com/science/article/abs/pii/S0268401219317311> (Access data: 15.04.2024).

5. Smith, M. The ethical application of biometric facial recognition technology / M. Smith, S. Miller // *AI & Soc*. – 2022. – № 37. – Pp. 167-175.

6. Kodasheva, G.S. Udalennaja biometricheskaja identifikacija v bankovskoj sfere Kazahstana kak chast' cifrovoj infrastruktury // *Finansovye aspekty tret'ej modernizacii jekonomiki Kazahstana: sb. materialov mezhdunar. nauchn.-praktich. konf.* – 2021. – S. 405-413.

7. Karabekov, K.O. Sostojanie i tendencii kiberprestupnosti v Rossijskoj Federacii i Respublike Kazahstan / K.O. Karabekov // *Nauchnyj vestnik Omskoj akademii MVD Rossii*. – 2024. – № 30 (2 (93)). – S. 106-112.

8. Luk'janchikov, A.I. Princip raboty sistem raspoznavaniya lic i osobennosti ih primeneniya pri obrabotke videopotoka v real'nom vremeni / A.I. Luk'janchikov i dr. // *Informatika i vychislitel'naja tehnik a i upravlenie. Serija: Estestvennyye i tehnicheckie nauki*. – 2023. – № 5. – S. 76-83.

9. Grechanyj, S.A. Raspoznavanie lic v sovremennyh sistemah videonabljudeniya. Na primere oborudovaniya TM / S.A. Grechanyj, N.Ju. Fedina, M.V. Hramykov // *Ohrana, bezopasnost', svjaz'*. – 2020. – № 5-1. – S. 63-68.

10. Utegen, D. Tehnologija raspoznavaniya lic i obespechenie bezopasnosti biometricheskikh dannyh: komparativnyj analiz modelej pravovogo regulirovaniya / D. Utegen, B.Zh. Rahmetov // *Journal of Digital*



Technologies and Law. – 2023. – № 1 (3). – S. 825-844.

11. Jacucenko, V.V. Problemy i perspektivy vnedrenija cifrovyyh tehnologij v dejatel'nost' organov prokuratury / V.V. Jacucenko // Aktual'nye problemy rossijskogo prava. – 2021. – № 11 (132). – S. 187-193.

12. Kindt, E. A first attempt at regulating biometric data in the European Union // Regulating biometrics: Global approaches and urgent questions. – 2020. – Pp. 62-69.

13. Alsaadi, I.M. Study on most popular behavioral biometrics, advantages, disadvantages and recent applications: A review / I.M. Alsaadi // International journal of scientific & technology research. – 2021. – № 10. – Pp. 15-21.

14. Stylios, I., Behavioral biometrics & continuous user authentication on mobile devices: A survey / I. Stylios, et al. // Information Fusion. – 2021. – № 66. – Pp. 76-99.

15. Grushin, F.V. Fotoizobrazhenie i opisanie primet osuzhdennyh k lisheniju svobody kak vid personal'nyh dannyh, podlezhashhih obrabotke v ugovovno-ispolnitel'noj sisteme Rossii / F.V. Grushin, A.Ju. Sivcova // Vestnik Samarskogo juridicheskogo instituta. – 2022. – № 1 (47). – S. 45-51.

16. Soldatova, V.I. Zashhita personal'nyh dannyh v uslovijah primenenija cifrovyyh tehnologij / V.I. Soldatova // Lex russica. – 2020. – № 2 (159). – S. 33-43.

АВТОРЛАР ТУРАЛЫ МӘЛІМЕТТЕР / СВЕДЕНИЯ ОБ АВТОРАХ / INFORMATION ABOUT AUTHORS

Алмас Мұратұлы Әміров – Қазақстан Республикасы Бас прокуратурасының жанындағы Құқық қорғау органдары академиясының докторанты, заң ғылымдарының магистрі, e-mail: han1k1986@mail.ru.

Амиров Алмас Муратович – докторант Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан, магистр юридических наук, e-mail: han1k1986@mail.ru.

Amirov Almas Muratovich – Doctoral Student of the Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan, Master of Law, e-mail: han1k1986@mail.ru.

Шәкір Шамильевич Шаяхметов – Қазақстан Республикасы Сот Әкімшілігі Басшысының бірінші орынбасары, заң ғылымдарының кандидаты, доцент, e-mail: shayhmet@mail.ru.

Шаяхметов Шакир Шамильевич – Первый заместитель руководителя Судебной администрации Республики Казахстан, кандидат юридических наук, доцент, e-mail: shayhmet@mail.ru.

Shayakhmetov Shakir Shamilevich – First Deputy Head of the Judicial Administration of the Republic of Kazakhstan, Candidate of Law, Associate Professor, e-mail: shayhmet@mail.ru.