

3. Кодекс об административной ответственности Республики Узбекистан. URL: <https://lex.uz/ru/docs/97661#2392706> (дата обращения: 12.09.2022).
4. Положение о Министерстве по развитию информационных технологий и коммуникаций Республики Узбекистан утвержденного Постановлением Кабинета Министров от 1-мая 2018 г. № 318.
5. Барциц И.Н. Развитие потенциала государственного потенциала управления в России: Правовые условия и критерии эффективности. С. 28. URL: <https://cyberleninka.ru/article/n/razvitie-potentsiala-gosudarstvennogo-upravleniya-v-rossii-pravovye-usloviya-i-kriterii-effektivnosti> (дата обращения: 09.09.2022).
6. Сидоренко Э, Барциц И., Хисамова З. Эффективность цифрового государственного управления: теоретические и прикладные аспекты // Вопросы государственного и муниципального управления. 2019. № 2.
7. Смотрицкая И. И., Черных С. И. Современные тенденции цифровой трансформации государственного управления // Вестник Института экономики Российской академии наук. 2018. № 5. С. 23.
8. Смотрицкая И. И. Государственное управление в условиях развития цифровой экономики: стратегические вызовы и риски // Цифровая экономика. 2018. DOI: 10.24411/2071-6435-2018-10037
9. Тихомиров Ю. А. Управление на основе права. М., 2007. С. 8.
10. Рейтинг стран по уровню развития электронного правительства. URL: <https://nonews.co/directory/lists/countries/e-government>. (дата обращения: 08.09.2022).
11. Реформирование системы государственного управления. URL: https://minjust.uz/ru/library/own_publications/71169/ (дата обращения: 08.09.2022).
12. Эффект кобры описывает, как стимулы, предназначенные для улучшения системы, могут привести к непредусмотренным – а иногда и к извращенным – последствиям, которые могут усугубить проблемы, а не исправить их. URL: <https://tospeople.com/2022/05/effekt-kobry/> (дата обращения: 07.09.2022).

Д. У. Мухамеджанова,

Заместитель директора Высшей школы права,
Университет КАЗГЮУ имени М. С. Нарикбаева

БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ В КАЗАХСТАНЕ И РИСКИ, СВЯЗАННЫЕ С ПРАКТИКОЙ ЕЕ ПРИМЕНЕНИЯ

Аннотация. В данной статье проведен анализ законодательства Республики Казахстан по части сбора и защиты биометрических данных, дактилоскопической и геномной регистрации. Рассмотрены примеры применения биометрической аутентификации в мировой практике, а также некоторые виды утечек персональных данных, угроз информационной безопасности и приватности. Также рассмотрена практика использования систем биометрической идентификации в Казахстане и практика применения международных стандартов в области биометрической идентификации в целях предотвращения нарушений прав человека. В заключении

представлены рекомендации по снижению рисков, связанных с угрозами утечек чувствительной информации, указаны пробелы действующего законодательства, отсутствие отдельного закона о защите биометрических данных в Республике Казахстан и другие аспекты, связанные с пробелами регулирования биометрических данных.

Ключевые слова: идентификация, биометрическая аутентификация, биометрические данные, приватность, персональные данные, неприкосновенность частной жизни

BIOMETRIC AUTHENTICATION IN KAZAKHSTAN AND RISKS ASSOCIATED WITH THE PRACTICE OF ITS APPLICATION

Abstract. This article will analyze the legislation of the Republic of Kazakhstan regarding the collection and protection of biometric data, fingerprint and genomic registration. The article will consider examples of the use of biometric authentication in the world and some types of personal data leaks, threats to information security and privacy. The practice of using biometric identification systems in Kazakhstan and the practice of applying international standards in the field of biometric identification in order to prevent human rights violations will also be discussed. In conclusion, recommendations to reduce the risks associated with the threats of leaks of sensitive information, the gaps in the current legislation, the absence of a separate law on the protection of biometric data in the Republic of Kazakhstan and other aspects related to the gaps in the regulation of biometric data will be indicated.

Keywords: Identification, Biometric authentication, Biometric data, Personal data, Privacy

Введение. Биометрическая идентификация, производимая при помощи биологических признаков субъекта, используется в различных сферах: при получении государственных услуг; документов, удостоверяющих личность с привязкой к биометрическим данным; паспорта с поддержкой NFC; цифровых документов; при установлении камер с функцией распознавания лица; проведении платежных операций, бесконтактной оплаты и др. Идентификация личности при помощи биометрии существенно повысила эффективность процесса экономии затрат, предотвращения мошеннических операций и коррупции, раскрытия преступлений, криминалистических расследований, она способствует расширению функций, направленных на упрощение и оптимизацию получения услуг.

В 2016 г. был принят Закон Республики Казахстан «О дактилоскопической и геномной регистрации», дата вступления в силу, которого было запланирована на 1 января 2021 г. [1]. Однако начало действия данного закона в части дактилоскопической регистрации было перенесено на 1 января 2023 г., перенос сроков Министерством внутренних дел Республики Казахстан было обусловлено пандемией COVID-19 и опасением развития эпидемиологической ситуации.

Дактилоскопии отпечатков пальцев будут подлежать граждане Республики Казахстан, достигшие 16-летнего возраста, иностранные граждане, лица без граж-

данства, постоянно проживающие в стране, иммигранты, прибывшие в Республику Казахстан в качестве домашних работников, иностранцы и лица без гражданства, подлежащие выдворению за пределы Республики Казахстан.

При получении паспорта и только с согласия и в присутствии опекуна дети в возрасте от 12 до 16 лет будут проходить добровольную процедуру сдачи отпечатки пальцев. Дети, не достигшие 12 лет, а также лица с физическими недостатками, такими как отсутствие всех пальцев либо папиллярных узоров на ногтевых фалангах всех пальцев на обеих рук не подлежат дактилоскопической регистрации [2].

Помимо всеобщей и обязывающей процедуры дактилоскопической регистрации, в 2020 г. в Казахстане вступил в силу Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан «Об утверждении Правил сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг» [3]. Также одним из существенных шагов применения биометрических данных в качестве элементов защитных действий при идентификации клиента стал Закон «О платежах и платежных системах», в котором было обозначено использование Face ID для входа в мобильный банкинг при удаленной выдаче кредитов и получении доступа к другим банковским и финансовым услугам, в том числе электронной цифровой подписи, шифрования, биометрических данных [4].

Также понятие биометрической идентификации как включающее комплекс мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков было включено в 2019 г. в постановление Правления Национального Банка Республики Казахстан в Правилах предоставления микрокредитов электронным способом [5]. В них также предусмотрены случаи отсутствия удаленной идентификации по биометрическим параметрам (Face ID).

Существенным шагом в развитии инициатив по введению и созданию инновационной экосистемы стало внедрение программы «Цифровой Казахстан», в рамках которой в развитие цифровых технологий, в том числе и биометрических данных, вовлечен малый и средний бизнес [6].

Остановимся на относительно недавно принятом документе в Республике Казахстан – Программе создания Национальной платформы цифровой биометрической идентификации на 2021–2024 гг. [7]. Инициатива связана с созданием национальной платформы цифровой биометрической идентификации, которая станет основой для дальнейшего безопасного, эффективного, удобного для граждан и бизнеса внедрения цифровых технологий. Программа должна способствовать обеспечению управлению собственными персональными данными, конкурентному развитию цифровых услуг, способствовать достижению целей экономического и социального развития. Программа направлена на процесс идентификации личности субъекта, созданию определенного жизненного цикла идентификации, к примеру, при оказании банковских услуг, платежных операций и др. [7].

Вышеуказанная подборка НПА подчеркивает наличие различных документов, регулирующих способы применения биометрической аутентификации, однако следует обратить внимание на то, что в законодательстве Казахстана отсут-

ствует отдельный нормативный правовой акт, регулирующий процесс обработки и хранения биометрических данных. Перечень биометрических данных носит сжатый характер описания. Отмечается дробление процесса применения биометрических данных в различных сферах.

Основная часть. В отличие от Казахстана в ряде государств приняты отдельные законы, регулирующие процесс обработки и хранения биометрических данных.

Если рассмотреть практику определения биометрических данных в рамках Европейского союза, можно привести пример ограничения использования биометрических данных Европейским парламентом. Так как использование систем искусственного интеллекта может привести к массовой слежке, нарушению ключевых принципов ЕС о пропорциональности и необходимости, внесено предложение по Регламенту об искусственном интеллекте [8], в том числе требующее полного запрета на алгоритмы использования искусственного интеллекта для автоматического распознавания лиц в общественных местах, по походке, отпечаткам пальцев, ДНК, голосу и иным биометрическим данным, создающим чрезвычайно высокие риски для основных прав и свобод.

Данный опыт ЕС по запрету алгоритмов использования искусственного интеллекта связан с наличием опыта использования технологии распознавания лиц правительством государств, нацеленных на чрезмерный контроль и установление определенных ограничений прав человека. К примеру, в Иранском правительстве запланировано использование камер с функцией распознавания лиц в общественном транспорте для выявления женщин, которые не соблюдают строгий закон о ношении хиджаба, режим предусматривает карательные меры по части ношения женской одежды. С 2015 г. иранское правительство поэтапно внедрило базу удостоверений личности, включающий биометрические данные, такие как сканирование радужной оболочки глаза, отпечатки пальцев и изображение лица. Общественники выражают опасения, что чувствительная информация будет использована для идентификации людей, которые нарушают обязательный дресс-код [9].

В Российской Федерации прорывом в части сбора биометрических данных стала Единая биометрическая система (ЕБС). В октябре 2018 г. оператор представил мобильное приложение «Ключ Ростелеком», позволяющее клиентам банков проходить удаленную биометрическую идентификацию при помощи смартфона. Система включает акцент на банковское обслуживание, ЕБС при идентификации, параметры определения данных изображения лица человека, полученные с помощью фото- и видеоустройств, данные голоса человека, полученные с помощью звукозаписывающих устройств [10]. Обеспечение безопасности, упрощение проведения платежных операций, к сожалению, не может служить в полной мере защитой от рисков, связанных с покупкой и продажей чувствительных данных. Повсеместный сбор биометрических данных может повлиять также на тотальный контроль над людьми. Обладание обширными базами идентификаторов и чрезмерными полномочиями может привести к нарушению баланса между обеспечением безопасности и защитой прав человека

Заключение. Применение биометрических данных создает существенные опасения и угрозы, способствующие нарушению прав человека, в частности права на неприкосновенность частной жизни и защиту персональных данных [11].

Технологические достижения позволяют при помощи биометрических данных устанавливать повсеместный контроль, это создает предпосылки для возникновения источников рисков и угроз приватности при операциях, связанных с обработкой классифицирующих биологических признаков. Данные проблемы могут оказать существенное влияние на личные свободы и права человека и, следовательно, должны подлежать оценке воздействия на защиту данных.

Следует более детально изучить и проанализировать опыт зарубежных государств, в частности, на способы досудебной и судебной защиты персональных данных, доступа к информации о самом себе, ситуаций, связанных с возможным злоупотреблением и получением избыточной информации, относящейся к субъекту.

Анализируя практику государств, внедривших биометрическую аутентификацию, следует вынести следующие рекомендации:

- уполномоченными органом, регулирующему сбор и обработку персональных данных, обеспечить мониторинг в отношении операторов государственного и частного сектора;
- недопущение избыточного сбора данных,
- ограничение сбора биометрических данных без письменного согласия субъекта;
- недопущение доступа к чувствительной информации правительствам или иным заинтересованным третьим лицам в контексте защиты основных прав и свобод человека,
- рассмотреть создание отдельного законодательства, регулирующего защиту биометрических данных в Казахстане, основанного на общепризнанных принципах защиты персональных данных и приватности.

Список литературы

1. Закон Республики Казахстан от 30 декабря 2016 года № 40-VI «О дактилоскопической и геномной регистрации» (с изменениями и дополнениями по состоянию на 01.07.2021). URL: https://online.zakon.kz/Document/?doc_id=33276266 (дата обращения: 19.09.2022).
2. Обязательная дактилоскопия казахстанцев: зачем она нужна и как это работает? – URL: <https://cabar.asia/ru/zachem-vvoditsya-obyazatel'naya-daktiloskopiya-kazahstantsev> (дата обращения: 19.09.2022).
3. Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НК «Об утверждении Правил сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг». URL: https://online.zakon.kz/Document/?doc_id=32282402 (дата обращения: 19.09.2022).

4. О платежах и платежных системах. URL: <https://zakon.uchet.kz/rus/docs/Z1600000011> (дата обращения: 19.09.2022); об утверждении Государственной программы «Цифровой Казахстан»: Постановление Правительства Республики Казахстан от 12.12.2017 № 827. URL: <https://adilet.zan.kz/rus/docs/P1700000827> (дата обращения: 03.09.2022).

5. Выдача онлайн-микрокредитов без биометрической аутентификации будет запрещена. URL: https://online.zakon.kz/Document/?doc_id=36831547 (дата обращения: 19.09.2022).

6. О платежах и платежных системах. URL: <https://zakon.uchet.kz/rus/docs/Z1600000011> (дата обращения: 19.09.2022).

7. Отчет Министерства цифрового развития, инноваций и аэрокосмической промышленности РК «Об утверждении Программы создания Национальной платформы цифровой биометрической идентификации на 2021–2024 годы». URL: <https://legalacts.egov.kz/report?id=13895562> (дата обращения: 19.09.2022).

8. European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe's digital future. URL: <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence> (дата обращения: 19.09.2022).

9. Iranian authorities plan to use facial recognition to enforce new hijab law. URL: <https://www.theguardian.com/global-development/2022/sep/05/iran-government-facial-recognition-technology-hijab-law-crackdown> (дата обращения: 19.09.2022).

10. Биометрия в России: правовое регулирование и практика применения. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Biometrics-in-Russia#part3 (дата обращения: 19.09.2022).

11. Значимости проекта БиометрияKZ в академическом сообществе. URL: <https://erkindikqanaty.com/tpost/bj0n4n2vx1-znachimosti-proekta-biometriyakz-v-akade> (дата обращения: 19.09.2022).

Ю. А. Немчик,

кандидат военных наук,

Московский областной филиал Российской академии
народного хозяйства и государственной службы
при Президенте Российской Федерации

ТЕОРЕТИКО-ПРАВОВЫЕ ОСНОВЫ СОЗДАНИЯ И СОВЕРШЕНСТВОВАНИЯ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА В ИНТЕРЕСАХ СОЦИАЛЬНОГО РАЗВИТИЯ РОССИИ

Аннотация. Эта обзорная статья показывает, на каких теоретико-правовых основах в России начали применяться и совершенствоваться информационно-коммуникационные технологии в процессе выполнения органами государственного управления функций по реализации властных полномочий, как изменялись цели и задачи правовой базы концепции создания Электронного правительства за период функционирования. Проанализированы основные итоги концепции электрон-