**ДАЙЫРБЕКОВ Руслан Токтоналиевич**
*Евразийский Цифровой Фонд (Eurasian Digital Foundation), основатель, GDPR DPP (Data Privacy Professional) (050020, Алматы, Казахстан, Жолдасбекова 24/44 E-mail: rdairbekov@yandex.ru)*

# БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ В КАЗАХСТАНЕ: ПРАВОВЫЕ ОСОБЕННОСТИ ОБРАБОТКИ БИОМЕТРИЧЕСКИХ ДАННЫХ ГРАЖДАН

***Аннотация.*** *В Казахстане набирает обороты инициатива по внедрению технологий биометрической идентификации граждан. Для обеспечения безопасности, упрощения и развития цифровых услуг, в том числе государственных, социальных и коммерческих, предполагается построить модель удаленной идентификации, в том числе основанной на различных биометрических показателях.*

*В рамках реализации государственной программы «Цифровой Казахстан» предполагается внедрение цифрового идентификационного механизма, который по замыслу законодателя станет основополагающей инфраструктурой, которая позволит построить универсальную цифровую среду для взаимодействия и коммуникаций между финансовыми институтами, клиентами, государственными органами и организациями, что позволит качественно повысить уровень и эффективность оказания финансовых, государственных и других услуг[119]. Модель предполагает идентификацию клиентов с использованием базы данных государственных и коммерческих компаний.*

[119] Государственная Программа «Цифровой Казахстан» утверждена постановлением Правительства Республики Казахстан от 12 декабря 2017 года № 827.
https://adilet.zan.kz/rus/docs/P1700000827



*Биометрические системы призваны обеспечить распознавание человека с использованием его биологических и физиологических характеристик, таких, например, как отпечатки пальцев, радужная оболочка глаза, лицо, ДНК и т.д. Само по себе планируемое построение модели удаленной идентификации, в том числе основанной на различных биометрических показателях в Казахстане можно только приветствовать. Это тем более важно в период построения универсальной цифровой среды для предсказуемости и правовой определённости этого процесса.*

*Тем не менее, для того, чтобы в полной мере реализовать потенциал биометрических технологий, государству необходимо решать вопросы, связанные с защитой лиц, идентифицируемых такими системами, добиваясь, чтобы сбор, хранение и использование биометрических данных велись в соответствии с международными стандартами в области прав человека, в том числе права на неприкосновенность частной жизни.*

***Ключевые слова:*** *права человека, цифровые технологии, биометрия, биометрическая идентификация, персональные данные, государственные услуги, частная жизнь.*

## Нормативно-правовая база

Анализируя процесс развития законодательства в сфере использования биометрии, во-первых, следует отметить, что правовое определение биометрической идентификации (аутентификации) было закреплено в национальном законодательстве в 2019 году. Так, в Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»[120] были внесены дополнения Законом Республики Казахстан от 25 ноября 2019 года № 272-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по

[120] Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»
https://adilet.zan.kz/rus/docs/Z1500000418

вопросам оказания государственных услуг»[121], которые, среди прочего, закрепили определение биометрической аутентификации, как *комплекса мер, идентифицирующих личность на основании физиологических и биологических неизменных признаков*.

Во-вторых, следует отметить Закон Республики Казахстан от 30 декабря 2016 года № 40-VI ЗРК «О дактилоскопической и геномной регистрации». Согласно, вышеуказанному закону дактилоскопическая и геномная регистрация проводится в целях установления и (или) подтверждения личности на основе дактилоскопической или геномной информации[122]. Другими словами, в целях повышения эффективности системы государственной регистрации, согласно настоящему закону, органы внутренних дел должны, среди прочего, осуществлять сбор отпечатков пальцев у граждан, иностранных граждан и лиц без гражданства, постоянно проживающих в Казахстане. В свою очередь, по замыслу законодателей, наличие геномной базы данных позволит повысить раскрываемость преступлений и более успешно вести их профилактику.

Закон «О дактилоскопической и геномной регистрации» вступил в силу 1 января 2021 года. Однако, в декабре 2020 года Министерство внутренних дел Республики Казахстан совместно с заинтересованными государственными органами внесло в Парламент предложение о переносе срока введения в действие отдельных норм закона в части дактилоскопической регистрации на 1 января 2023 года[123].

[121] Законом Республики Казахстан от 25 ноября 2019 года № 272-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам оказания государственных услуг» https://adilet.zan.kz/rus/docs/Z1900000272

[122] Закон Республики Казахстан от 30 декабря 2016 года № 40-VI ЗРК «О дактилоскопической и геномной регистрации» https://adilet.zan.kz/rus/docs/Z1600000040

[123] https://tengrinews.kz/kazakhstan_news/sdachu-otpechatkov-paltsev-kazahstantsami-perenesli-2023-god-424900/



Кроме этого, в Казахстане наблюдается рост использования биометрии в сфере предоставления финансовых услуг. Согласно, «Правилам оказания банками и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг», утвержденными постановлением Национального Банка Республики Казахстан от 31 августа 2016 года № 212, биометрическая идентификация, наряду с электронной цифровой подписью, отнесена к одному из способов идентификации физических лиц при предоставлении электронных платежных услуг[124].

**Биометрия при оказании государственных услуг**

В настоящее время, лишь посредством идентификации человека (определение его социального и правового статуса) государственные служащие и иные должностные лица удостоверяют его право на получение государственных и муниципальных услуг. Законодательное закрепление механизма биометрической идентификации при оказании государственных услуг, как средства аутентификации граждан для совершения юридически значимых действий в электронной форме, безусловно, является существенной вехой в развитии отечественного «цифрового» законодательства.

В 2020 году, для нормативно-правового обеспечения внедрения механизма биометрической идентификации граждан при оказании государственных услуг, Правительством Республики Казахстан были внесены изменения и дополнения в ряд отраслевых законов, а также приняты отдельные подзаконные акты.

25 июня 2020 года Президент Республики Казахстан подписал Закон № 347-VI «О внесении изменений

[124] «Правила оказания банками и организациями, осуществляющими отдельные виды банковских операций, электронных банковских услуг», утвержденные постановлением Национального Банка Республики Казахстан от 31 августа 2016 года № 212 https://adilet.zan.kz/rus/docs/V1600014337

и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» (далее — «Закон о регулировании цифровых технологий»)[125]. Так, согласно вышеуказанным дополнениям в Закон Республики Казахстан от 15 апреля 2013 года «О государственных услугах»[126], уполномоченный орган в сфере оказания государственных услуг (АО «Государственная корпорация «Правительство для Граждан») наделен правом *осуществлять сбор, обработку и хранение биометрических данных физических лиц в сфере оказания государственных услуг, а также правом ведения биометрической базы данных физических лиц, используемой для биометрической аутентификации в рамках оказания государственных услуг*.

Кроме этого, в компетенцию уполномоченного органа (АО «Государственная корпорация «Правительство для Граждан») вошла разработка и утверждение правил сбора, обработки и хранения биометрических данных в сфере оказания государственных услуг для биометрической аутентификации физических лиц по согласованию с уполномоченным органом в сфере защиты персональных данных (Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан).

Вышеуказанные правила не заставили себя долго ждать, и 27 октября 2020 года Министр цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан своим приказом утвердил «Правила сбора, обработки и хранения биометрических данных

[125] Закон № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий»
https://adilet.zan.kz/rus/docs/Z2000000347

[126] Закон Республики Казахстан от 15 апреля 2013 года «О государственных услугах»
https://adilet.zan.kz/rus/docs/Z1300000088



физических лиц для их биометрической аутентификации при оказании государственных услуг»[127].

Согласно правилам, сбор и обработка биометрических данных для аутентификации при оказании государственных услуг, производится у физических лиц, достигших восемнадцатилетнего возраста, на добровольной основе. Заявление гражданина о желании уничтожения его биометрических данных и исключения их из базы подаются в любой городской (районный) отдел обслуживания населения филиалов АО «Государственная корпорация «Правительство для Граждан» по областям и городам Нур-Султан, Алматы, Шымкент. Хранение и передача биометрических данных осуществляется с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности в соответствии со стандартом Республики Казахстан СТ РК 1073–2007 «Средства криптографической защиты информации. Общие технические требования».

Наконец, приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 13 октября 2020 года № 383/НҚ были внесены дополнения в «Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан»[128]. Таким образом, был дополнен существующий

[127] «Правила сбора, обработки и хранения биометрических данных физических лиц для их биометрической аутентификации при оказании государственных услуг», Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2020 года № 406/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 октября 2020 года № 21547
https://adilet.zan.kz/rus/docs/V2000021547

[128] «Правила выдачи, хранения, отзыва регистрационных свидетельств и подтверждения принадлежности и действительности открытого ключа электронной цифровой подписи удостоверяющим центром государственных органов Республики Казахстан», Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 июня 2015 года № 727. Заре-

подход требований к подтверждению принадлежности и действительности электронной цифровой подписи (далее — «ЭЦП») в Казахстане. Применение биометрической идентификации лица граждан узаконено как дополнительный способ аутентификации при получении регистрационного свидетельства ЭЦП, а также, при осуществлении пользователем доступа к закрытому ключу облачной ЭЦП, где биометрическая идентификация используется при двухфакторной аутентификации.

Применение биометрических технологий в Казахстане приобретает все более повсеместный характер, и одновременно с этим общественность задается вопросом: «*Какие процессуальные гарантии по соблюдению права человека на неприкосновенность личной жизни и конфиденциальность его персональных данных, предусмотрело законодательство при использовании биометрических технологий»?*

**Биометрия и права человека**

Любая часть государственной информационной системы, в которой используются биометрические данные, может стать объектом внешней электронной/кибератаки, физического нападения, внутреннего вмешательства или саботажа в результате неправомерных действий персонала. Противоправное использование биометрических данных (как по ошибке, так и в злонамеренных целях) может привести к неблагоприятным правовым последствиям для отдельных лиц или нанести им иной ущерб. Следовательно, с одной стороны, необходимо создать многоуровневую систему безопасности для защиты операционной среды, аппаратных средств, программного обеспечения, сети связи и хранимых данных, а с другой стороны, в законодательстве следует предусмотреть надлежащие средства

гистрирован в Министерстве юстиции Республики Казахстан 16 октября 2015 года № 12181. https://adilet.zan.kz/rus/docs/V1500012181



правовой защиты, если при обработке биометрических данных нарушаются права человека, в том числе права на неприкосновенность личной жизни. Как справедливо отмечает Талапина Э. В., «*проблематика прав человека может способствовать выработке целостного представления о регулировании новых технологий. Права человека могут стать «маяками» для регулирования информационно-коммуникационных технологий, указывая, какие цели должны быть достигнуты и какой вред должен быть предотвращен в соответствии с принципом пропорциональности*»[129].

В Казахстане планируется создать единую платформу биометрических данных, но без закрепления нормативно-правовых и технических требований к базам биометрических данных, а также, требованиям по проведению оценки воздействия на неприкосновенность частной жизни, эффективность рассматриваемых процедур управления биометрическими идентификационными данными, ставится под сомнение.

Государствам рекомендуется эксплуатировать свои биометрические системы в соответствии с международными техническими стандартами. В соответствии, с «Правилами классификации объектов информатизации и классификатор объектов информатизации», утвержденными Приказом Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135[130], *государственная система биометрической идентификации является объектом информатизации и от-*

[129] Талапина Э. В. Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. 2019.
Т. 14. № 3. С. 122–146. DOI: 10.35427/2073–4522–2019–14–3-talapina
https://cyberleninka.ru/article/n/evolyutsiya-prav-cheloveka-v-tsifrovuyu-epohu/viewer

[130] «Правила классификации объектов информатизации и классификатор объектов информатизации», Приказ Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135. https://adilet.zan.kz/rus/docs/V1600013349

*носится к общесистемному программному обеспечению*. Уполномоченный орган в области информатизации при определении требований, применимых к биометрической системе, в соответствии с едиными требованиями в области информационно-коммуникационных технологий и обеспечения информационной безопасности, классифицирует биометрическую систему как следующую категорию объектов информатизации: «Система биометрической идентификации (BIDS, Biometric Identification System)».

В целях приведения рассматриваемого объекта информатизации (государственная система биометрической идентификации) в соответствие с международными стандартами, следует обратить внимание регулятора в области информатизации, и соответственно, отразить в действующем законодательстве международный стандарт ISO/IEC 2382–37:2017(E) (Information technology — Vocabulary — Part 37: Biometrics)[131] Международной организации по стандартизации (ISO), которая приводит разработанные международными или национальными организациями стандарты в соответствие требованиями в таких областях, как неприкосновенность частной жизни и законодательство о защите данных.

Биометрические системы сопряжены со сложным комплексом угроз, который продолжает расширяться по мере дальнейшего внедрения биометрических технологий. Создание всеобъемлющей классификации всех уязвимостей и рисков в этой области описаны в стандарте ИСО/МЭК 30107–2_2017[132].

## Заключение

В целях создания эффективной нормативно-

[131] Международный стандарт ISO/IEC 2382–37:2017(E) (Information technology — Vocabulary — Part 37: Biometrics). https://www.iso.org/standard/66693.html

[132] Международный стандарт ИСО/МЭК 30107–2_2017. https://www.iso.org/ru/standard/67380.html



правовой базы, устанавливающей режим правомерного использования биометрических данных, контроля и ответственности за деятельностью государственных органов по соблюдению процедур сбора, хранения и использования биометрических персональных данных граждан, следует рассмотреть возможность внесения корректив в законодательство Республики Казахстан, отражающих современные виды применения оценок воздействия на неприкосновенность частной жизни.

Оценка воздействия на неприкосновенность частной жизни (PIA)[133], является частью концепции «проектируемой конфиденциальности»[134], используемой для управления данными в государственных и коммерческих организациях. Процедура проведения PIA обеспечивает соответствие правовым и регуляторным нормам неприкосновенности частной жизни посредством выявления потенциальных рисков и разработки стратегий смягчения этих рисков и управления ими. Права человека могут стать «объединяющей целевой перспективой» (“unifying purposive perspective”) при определении отношения к различным технологиям, что предполагает анализ того, соответствует или не соответствует их использование фундаментальным правам человека, таким как достоинство, частная жизнь, равенство, свобода[135].

Основанный на принципах соблюдения прав человека подход к использованию биометрических технологий

[133] Сводный отчет о первой оценке воздействия на права человека, подготовленный для корпорации ICANN Löning — Human Rights and Responsible Business 05.2019. https://www.icann.org/en/system/files/files/summary-report-hria-15may19-ru.pdf

[134] Privacy by Design 7 основополагающих принципов, Энн Кавукиан (Ann Cavoukian), Ph. D. Уполномоченный по вопросам информации и защиты конфиденциальности, Онтарио, Канада. https://online.zakon.kz/document/?doc_id=31633216#pos=1;-16

[135] См.: Brownsword R., Scotford E., Yeung K. Law, Regulation, and Technology: The Field, Frame, and Focal Questions // The Oxford Handbook of Law, Regulation and Technology / Ed. by R. Brownsword, E. Scotford, K. Yeung. P. 3–40.

должен предусматривать применение процессуальных гарантий и эффективный контроль за их соблюдением.

### Библиографический список


1. *Архипов В. В.* Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2. С. 52–68.
2. *Бусурманов Ж. Д.* Евразийская концепция прав человека. Астана: Изд-во КазГЮУ, 2010.
3. *Степин В. С.* Права человека в эпоху глобализации и диалога культур // Всеобщая декларация прав человека: универсализм и многообразие опытов. М.: Институт государства и права РАН, 2009. С. 14–31.
4. *Талапина Э. В.* Эволюция прав человека в цифровую эпоху // Труды Института государства и права РАН / Proceedings of the Institute of State and Law of the RAS. 2019. Т. 14. № 3. С. 122–146. DOI: 10.35427/2073–4522–2019–14–3-talapina.
5. *Терещенко Л. К.* Государственный контроль в сфере защиты персональных данных // Право. Журнал Высшей школы экономики. 2018. № 4. С. 142–161. DOI: 10.17323/2072–8166.2018.4.142.161.
6. *Brownsword R., Scotford E., Yeung K.* Law, Regulation, and Technology: The Field, Frame, and Focal Questions // The Oxford Handbook of Law, Regulation and Technology / Ed. by R. Brownsword, E. Scotford, K. Yeung. New York: Oxford University Press, 2017. P. 3–40. DOI: 10.1093/oxfordhb/9780199680832.013.1
7. *Sartor G.* Human Rights and Information Technologies // The Oxford Handbook of Law, Regulation and Technology / Ed. by R. Brownsword, E. Scotford, K. Yeung. New York: Oxford University Press, 2017. P. 424–450. DOI: 10.1093/oxfordhb/9780199680832.013.79




**ШАБЛИНСКИЙ Илья Георгиевич**
*Национальный исследовательский университет «Высшая школа экономики», факультет права, доктор юридических наук, профессор, ассоциированный член Кафедры ЮНЕСКО НИУ ВШЭ*
*(109028, Москва, Б. Трехсвятительский пер., 3;*
*тел.: +7495–772–9590; email: ishablin@hse.ru)*

# БЛОКИРОВКА ИНТЕРНЕТ-РЕСУРСОВ: СУДЕБНАЯ ПРАКТИКА

**Аннотация.** *В статье рассматривается и обобщается судебная практика по делам, связанным с использованием новых информационных технологий. Объектом исследования являются в основном решения российских судов (общей юрисдикции и арбитражных) и Европейского Суда по правам человека. Дела, связанные с применением новых информационных технологий, вообще, можно уже выделить в отдельный блок, но в данной статье рассматривается судебная практика по такой категории дел как блокировка интернет-ресурсов. В статье констатируется, что в эпоху бурного развития новых информационных технологий государства в лице специальных служб и уполномоченных государственных органов предпринимают беспрецедентные усилия для того, чтобы и в рамках новых информационных отношений сохранить хотя бы частичный контроль за деятельностью новых акторов (блогеров, интернет-СМИ, интернет-платформ и т.д.). При этом они достаточно часто встречают полное понимание судов.*

*Среди норм, регулирующих новую сферу отношений, достаточно часто встречаются (а в Российской Федерации доминируют) нормы ограничительные и запретительные. Возникавшие конфликты национальными судами нередко разрешались не в пользу граждан. В этой связи основания для озабоченности у юристов, занимающихся защитой прав, связанных с новыми информационными технологиями, остаются.*