

Научная статья
УДК 342.7
doi: 10.17223/15617793/476/28

Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом

Светлана Сергеевна Кузнецова^{1, 2}, Артур Николаевич Мочалов^{1, 3},
Марат Сабирьянович Саликов^{1, 4}

¹Уральский государственный юридический университет, Екатеринбург, Россия

²kss001@usla.ru

³artur.mochalov@usla.ru

⁴kp@usla.ru

Аннотация. На основе сравнительного изучения правового регулирования биометрической идентификации в США, Китае и Европейском союзе выделены три модели регулирования. В основе каждой из них лежит собственная конституционно-правовая концепция установления баланса между правами личности и публичными интересами. Дается оценка состоянию российского законодательства в данной сфере регулирования с точки зрения конституционно-правовых гарантий прав человека, в частности неприкосновенности частной жизни.

Ключевые слова: биометрическая идентификация, биометрическая информация, биометрические персональные данные, Интернет, права человека, неприкосновенность частной жизни

Источник финансирования: исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 18-29-16204.

Для цитирования: Кузнецова С.С., Мочалов А.Н., Саликов М.С. Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. С. 257–267. doi: 10.17223/15617793/476/28

Original article
doi: 10.17223/15617793/476/28

Biometric identification on the Internet: Trends of legal regulation in Russia and in foreign countries

Svetlana S. Kuznetsova^{1, 2}, Artur N. Mochalov^{1, 3}, Marat S. Salikov^{1, 4}

¹Ural State Law University, Yekaterinburg, Russian Federation

²kss001@usla.ru

³artur.mochalov@usla.ru

⁴kp@usla.ru

Abstract. The past few years saw the world's increased interest in biometric identification of Internet users. Biometric data differ from other identifiers: they are immutable and inalienable from their carriers, so any theft (including as a result of leakage) can lead to irreparable consequences. The aim of the article is to study the legal regulation of online biometric identification and processing of biometric data in the United States of America, China, and the European Union, as well as to assess the Russian legal regulation of this area in the light of world experience. For this, the authors use a comparative legal methodology. Each of the cases selected as research material illustrates one of the three regulatory models the authors identified. Each of the models is based on a certain constitutional concept of establishing a balance between users' private interests, on the one hand, and public interests, on the other. The US regulatory model is based on the establishment of minimum government guarantees of human rights observance in the processing of biometric data, while operators of Internet platforms remain with wide discretion in determining the procedure for processing biometric information. The Asian model, implemented, in particular, in China, proceeds from the priority of public interests over the privacy interests of individuals. States that implement such a model in their national legislation form centralized databases of subjects' biometric data, actively involving private Internet service providers in this process. The European model, which is based on the General Data Protection Regulation adopted in the European Union, on the contrary, proceeds from the recognition of the priority of the interests of the individual over public interests, establishing for this purpose strict rules regarding the processing of biometric data by Internet service providers and making it almost impossible to create centralized databases for

accumulation of such information. Analyzing the trends in Russian legislation, the authors come to the conclusion that legal regulation in Russia tends to the Asian model and note that its implementation is associated with significant risks to human rights and freedoms, including in connection with data leaks from biometric databases. The emphasis is made on the fact that Russia, unlike Asian countries, is a member of the Council of Europe and is bound by the human rights standards laid down in its international documents. These standards should be taken into account when legislating in this area.

Keywords: biometric identification, biometric information, biometric personal data, Internet, human rights, privacy

Financing: The study is supported by the Russian Foundation for Basic Research, Project No. 18-29-16204.

For citation: Kuznetsova, S.S., Mochalov, A.N. & Salikov, M.S. (2022) Biometric identification on the Internet: Trends of legal regulation in Russia and in foreign countries. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 476. pp. 257–267. (In Russian). doi: 10.17223/15617793/476/28

Число уникальных пользователей интернета достигло 4,66 млрд человек, что составляет 59,5% населения планеты¹. Цифровые следы, оставляемые человеком в Сети, «позволяют создать его цифровую копию, которая может существовать и действовать в киберфизическом пространстве независимо от того, по-прежнему ли существует данное лицо в реальном мире» [1. С. 147]. В начале существования глобальная Сеть была анонимной: ее протоколы не предусматривали передачи данных о пользователях, а действия последних не требовали раскрытия личности. Поэтому задача соотнесения «виртуальных личностей», скрывавшихся под никнеймами и аватарами, с реальными людьми не была актуальной. Однако с появлением цифровых платформ, на которых стало возможным заказывать банковские и страховые продукты, пользоваться государственными услугами, заключать договоры, возникла потребность в идентификации пользователей в качестве реально существующих субъектов права. Для этого стали использоваться «привязанные» к телефонным номерам коды и пароли, электронные подписи и т.д.

Биометрическая идентификация долгое время не получала распространения в интернет-среде, хотя именно она позволяет с высокой степенью достоверности соотносить виртуальную личность с физическим телом конкретного человека, стирая границу между офлайн- и онлайн-пространством. Причиной тому была высокая нагрузка на сети и устройства при обработке и хранении объемной и ресурсоемкой биометрической информации. Развитие технологий обработки данных (в том числе на основе искусственного интеллекта), появление информационных носителей нового поколения и «скоростных» сетей связи 4G и 5G открыло возможность широкого использования технологий удаленной биометрической идентификации и аутентификации.

В основе концепции юридически значимой идентификации лица на основе его физиологических данных лежат работы французского правоведа и криминалиста А. Бертильона, обосновавшего возможность использования индивидуальных внешних признаков человека для регистрации преступников [2]. Еще одним основоположником биометрической идентификации считается современник Бертильона английский исследователь Ф. Гальтон, впервые описавший статисти-

стический инструмент измерения и сопоставления антропометрических характеристик.

Сущность технологии биометрической идентификации и аутентификации заключается в создании «контрольного шаблона», представляющего собой срез некоторых индивидуальных антропометрических и физиологических характеристик конкретного человека (например, черт лица, рисунка радужной оболочки глаза, папиллярных узоров, рисунка вен, голоса, пропорций тела, геномной информации и т.д.) для последующего «узнавания» данного человека путем сопоставления его характеристик с записями, хранящимися в «контрольном шаблоне»². Несмотря на то, что узнавание человека по его внешним признакам (например, по лицу, фигуре, голосу) используется нами в повседневной жизни, о биометрической идентификации можно говорить в том случае, когда для этого применяются специальные программно-технические средства и лежащие в основе их действия алгоритмы.

По прогнозам экспертов, к 2024 г. порядка 66% населения мира будут использовать технологии биометрической идентификации в повседневной жизни. Катализатором развития удаленной биометрической идентификации в интернете послужила пандемия COVID-19: она стала активно использоваться, например, в сфере образования и в трудовых отношениях [3. Р. 7]. Биометрическая идентификация в системах видеонаблюдения с функцией распознавания лиц применяется государствами для обеспечения национальной безопасности, в том числе в качестве меры противодействия террористическим угрозам и массовым беспорядкам [4. С. 348]. Потребность в биометрической идентификации существенно возрастает и с развитием «интернета вещей» (*Internet of things*). В совокупности с технологиями анализа биометрических данных он находит практическое применение в приложениях для «умных домов», финансового сектора, промышленности, здравоохранения и т.д. [5. Р. 4461–4462].

Однако в отличие от паролей, которые легко сменить и которые не являются неотъемлемыми атрибутами личности, биометрические параметры, непосредственно связанные со своим субъектом-носителем, остаются неизменными на протяжении всей жизни человека; от них нельзя избавиться, их невозможно изменить [6. С. 38; 7. С. 110]. В случае

компрометации биометрических идентификаторов (неправомерного завладения третьими лицами, в том числе утечек данных из баз хранения контрольных шаблонов) будет крайне сложно найти им альтернативу и восстановить нарушенные права потерпевших субъектов. Эта угроза приобретает особую актуальность при использовании биометрической идентификации в интернете, предполагающей передачу соответствующих данных по сетям общего пользования. Благодаря технологиям «облачного» хранения информации обработка биометрических данных нередко приобретает трансграничный характер [8. Р. 1284–1285], а значит, потенциальный доступ к таким данным появляется у разных государств и частных операторов.

Указанная особенность биометрических данных (наряду с другими свойствами, такими как универсальность, уникальность, устойчивость [7, 9]) возводит проблемы регулирования их оборота в разряд конституционно-правовых. От того, насколько адекватным является правовое регулирование в данной сфере, напрямую зависит реализация человеком базовых конституционных прав, таких как право на неприкосновенность частной жизни и ее уважение, право на личную тайну, право на имя, идентичность, достоинство и т.д. Правовое регулирование во всяком случае должно включать установление стандартов безопасности биометрических данных и гарантии реализации индивидами своих прав в связи с оборотом биометрических данных, а также механизмы защиты от злоупотреблений. Изучению особенностей регулирования биометрической идентификации и обработки биометрических данных посвящен ряд недавно вышедших работ отечественных ученых [7, 9, 10]. Вместе с тем научный интерес представляет также опыт иностранных государств в правовом регулировании указанной сферы. Тенденции развития законодательства разных стран позволяют говорить о формировании трех моделей регулирования. Они будут рассмотрены в настоящей работе на примерах США, Китайской Народной Республики и Европейского союза.

Выбор материала для анализа является хотя и в некоторой степени произвольным (опыт других государств также достоин изучения), но вместе с тем не случайным: каждое из названных государственно-политических образований является в определенном смысле пионером в выработке соответствующей модели регулирования. Целью статьи является не только сравнительное изучение зарубежного опыта, но и оценка перспектив регулирования биометрической идентификации в законодательстве Российской Федерации в свете этого опыта.

Соединенные Штаты Америки. Первая модель правового регулирования биометрической идентификации и обработки биометрических данных представлена Соединенными Штатами Америки (США). Особенности правовой системы данной страны с учетом федеративной формы государственного устройства и ведущей роли судебных прецедентов обусловили отсутствие в ней единообразного регулирования данной сферы. Многие аспекты регламентации обработки

персональных данных (в том числе биометрических) здесь оставлены на усмотрение самих провайдеров интернет-услуг. Само же государственное регулирование остается крайне фрагментированным и ситуативным и нередко зависит от того, какую сферу представляет оператор, обрабатывающий биометрические данные.

Специальных законов, регулирующих оборот биометрической информации, на федеральном уровне не существует. На биометрические данные распространяются режимы защиты личных данных, устанавливаемые многочисленными отраслевыми законодательными актами, в основе которых лежат Первая и Четвертая поправки к Конституции. В частности, гарантируется правовая защита личных данных, обрабатываемых в рамках деятельности федеральных органов исполнительной власти (Закон «О частной жизни» (*Privacy Act*), Закон «О защите частной жизни водителя» (*The Driver's Privacy Protection Act*)), оказания услуг медицинского страхования и медицинской помощи (Закон «О мобильности и подотчетности медицинского страхования» (*Health Insurance Portability and Accountability Act*)), финансовых услуг (Закон «О финансовой модернизации» (*Financial Services Modernization Act*, также известный как «закон Грэмма–Лича–Блайли», Стандарт защиты данных в сфере использования карт оплаты (*Payment Card Industry Data Security Standard*)), телекоммуникационных услуг (Закон «О защите конфиденциальности видео» (*Video Privacy Protection Act*), Закон «О политике кабельной связи» (*Cable Communications Policy Act*) и др.), образовательных отношений (Закон «О правах семьи в сфере образования и частной жизни» (*Family Educational Rights and Privacy Act*)), а также личных данных несовершеннолетних пользователей интернета (Закон «О защите частной жизни детей онлайн» (*Children's Online Privacy Protection Act*)). Все указанные законы по-разному раскрывают содержание личных данных, распространяют действие на разные категории операторов и устанавливают различный порядок реализации субъектами своего права на защиту данных субъектом.

В Законе «О частной жизни», регламентирующем обработку личных данных граждан и постоянных резидентов США федеральными органами исполнительной власти, биометрические данные признаются частью так называемой записи (*record*) – «отдельного элемента, базы или категории информации об индивиде, которая хранится агентством, в том числе информация об его образовании, финансовых операциях, истории болезни, информация о судимостях, а также трудовой истории, и которая содержит его имя или идентификационный номер, символ или другую идентифицирующую личность информацию, такую как отпечаток пальца, аудиозапись голоса или фотографию». Данный закон предусматривает возможность раскрытия информации, содержащейся в записи, исключительно при наличии письменного согласия субъекта данных, однако не предусматривает аналогичного требования к иным формам обработки, например, к сбору информации. Отсутствие правового

го регулирования условий раскрытия информации частными субъектами «позволяет органам государственной власти обойти установленные законом ограничения путем обращения к информации из негосударственных центров обработки» [11. Р. 66].

Федеральное законодательство не предусматривает специальных требований к защите биометрической информации корпорациями и иными негосударственными объединениями. В частности, не существует единых требований к поставщикам интернет-услуг, в том числе порядка информирования пользователей о том, каким образом будет использоваться их личная информация [12. Р. 297] (за исключением случаев обработки данных о несовершеннолетних, а также данных пользователей при предоставлении им финансовых услуг). В литературе отмечается необходимость принятия федерального закона, регулирующего порядок обработки биометрических данных физическими и юридическими лицами в процессе осуществления коммерческой деятельности [13. Р. 161–192; 14. Р. 637–671; 15. Р. 328]. В 2020 г. в Сенат Конгресса США был внесен проект Национального закона о конфиденциальности биометрической информации (*National Biometric Information Privacy Act*), основывающийся на положительном опыте регулирования данной сферы на уровне отдельных штатов (в частности Иллинойса и Калифорнии). К настоящему моменту (декабрь 2021 г.) законопроект по-прежнему находится на рассмотрении Комитета Сената по судебной власти³.

Отсутствие на федеральном уровне единообразного регулирования порядка обработки и защиты биометрических данных в частноправовых отношениях, в том числе в онлайн-пространстве, обусловило принятие соответствующих нормативных правовых актов на уровне штатов. В основном региональное законодательство сосредоточивается на вопросах сбора и обработки данных с помощью цифровых устройств, а также данных, связанных с биометрическими идентификаторами личности [16. Р. 191]. В законодательной практике штатов сформировалось два подхода: первый предполагает принятие отдельного нормативного правового акта, предметом регулирования которого являются исключительно отношения по обработке и использованию биометрических данных (Иллинойс, Вашингтон, Техас); второй – создание механизмов защиты биометрической информации в рамках общего акта о защите персональных данных граждан штата (Калифорния, Нью-Йорк, Аризона, Луизиана, Орегон, Арканзас и др.).

Штаты, избравшие первый подход, гарантируют особый режим защиты биометрической информации, отличный от защиты иных персональных данных. Так, например, в соответствии с п. 15 закона штата Иллинойс «О конфиденциальности биометрической информации» (*Biometric Information Privacy Act*) 2008 г. обработка биометрических идентификаторов оператором возможна только в случае, если субъект данных дал письменное согласие на такую обработку. При этом запрещаются продажа, сдача в аренду или иные способы передачи биометрических данных с целью

получения прибыли. Законодательство штата Вашингтон и Техаса предоставляет субъекту обработки биометрической информации право ее использования в коммерческих целях только в случае получения на то согласия субъекта информации, однако законы не запрещают передачу биометрии третьим лицам, в том числе ее продажу, и не определяют форму получения согласия. Например, в Техасе оператор может продавать биометрические данные в случае «исчезновения или смерти» пользователя. В штате Вашингтон разрешено продавать биометрические данные третьим лицам, если последние «по контракту обещают» не раскрывать информацию [17. Р. 602]. В случае нарушения закона в Иллинойсе субъект может сам обратиться в суд. В двух других штатах предусмотрен публичный механизм защиты нарушенного права – путем обращения в суд прокурора штата. В числе жалоб, подаваемых в суды Иллинойса, присутствуют жалобы на использование систем видеонаблюдения; на сайты и приложения, которые используют программы распознавания лиц или требуют загрузки образцов голоса и т.д. [18. Р. 44].

Законы большинства штатов, которые избрали вторую модель регулирования защиты биометрических данных, часто применяют к биометрической информации общий режим защиты персональных данных. Закон штата Калифорния «О частной жизни потребителя» (*California Consumer Privacy Act*) 2018 г. не налагает на операторов особых обязательств в отношении биометрической информации, при этом предусматривает режим подразумеваемого согласия на обработку любых данных и их продажу. Закон гарантирует субъектам широкий перечень прав: получать информацию о собранных персональных данных, требовать удаления персональных данных, отказаться от продажи персональной информации. В законодательстве штата Арканзас определены лишь минимальные стандарты защиты персональных данных – обеспечение физической безопасности в разумном объеме, уничтожение информации в разумные сроки после достижения целей обработки, уведомление о факте утечки информации. В Орегоне закон направлен только на защиту персональной информации от кражи, однако не предоставляет субъекту информации права контролировать ее обработку.

Различается от штата к штату и содержание понятия биометрической информации. Закон Калифорнии «О частной жизни потребителя» трактует такую информацию предельно широко – «психологические, физические и поведенческие особенности личности, включая ДНК, которые могут быть использованы самостоятельно или в совокупности с иной идентифицирующей информацией с целью установления личности субъекта». Биометрической информацией признаются любые данные, из которых могут быть извлечены идентификаторы, такие как цифровое изображение лица, образец голоса, а также особенности нажатия клавиш или ритма, особенности походки или ее ритма, сон, состояние здоровья, информация о физических нагрузках и т.д. – все, что содержит идентифицирующую конкретного человека информацию. В

Иллинойсе в соответствии с разделом 10 названного выше закона штата биометрической признается любая информация, в основе которой лежит биометрический идентификатор человека – независимо от того, как эта информация собирается, конвертируется, хранится или передается. Под биометрическими идентификаторами понимаются сканы радужной оболочки, сетчатки глаза и руки, отпечатки пальцев, образец голоса, геометрия лица. Не признаются в качестве биометрических идентификаторов почерк, фотографии лица, демографические данные, описания внешности (рост, вес, цвет волос и глаз), татуировок, пробы анализов, отбираемые с целью научного исследования, а также донорские органы. Аналогичный подход используется в Техасе. В штате Вашингтон понятие биометрических идентификаторов еще уже. К таковым относятся «данные, полученные в результате автоматических измерений биологических характеристик человека, таких как отпечаток пальца, образец голоса, сетчатка глаза, радужная оболочка или другие уникальные биологические образцы или характеристики, которые используются для идентификации конкретного человека». Исключение из категории биометрических идентификаторов геометрии лица, а также признание в качестве таковых лишь информации, собираемой в процессе автоматических измерений, оставляют субъектов уязвимыми перед технологиями распознавания.

Вопрос о законности использования в интернет-приложениях алгоритмов распознавания лиц возник и в Иллинойсе. В решении по делу «Монро против Шаттерфлай» (*Monroy v. Shutterfly, Inc.*) 2017 г. суд округа признал тот факт, что «информация, полученная путем сканирования фотографии истца, не может быть признана в качестве биометрической, так как закона штата Иллинойс исключает фотографию из перечня биометрических идентификаторов». Однако суд не согласился с доводом ответчика, что биометрические идентификаторы могут быть получены только лично: «Отпечатки пальцев и сканы сетчатки глаза могут быть получены из изображений и фотографий... и даже если определенные виды биометрических идентификаторов не могут быть извлечены из фотографий в настоящий момент, учитывая скорость технологического развития, преждевременно говорить о том, что получение соответствующих данных не может быть реализовано в будущем». В результате суд признал наличие нарушений в действиях ответчика – администрации социальной сети «Шаттерфлай», которая не предоставила пользователям исчерпывающую информацию о порядке обработки биометрических идентификаторов и биометрической информации.

Китайская Народная Республика. Китайская Народная Республика (КНР) служит иллюстрацией следующей модели правового регулирования биометрической идентификации, особенностями которой являются создание централизованных государственных биометрических баз и широкое вовлечение в этот процесс как государственных органов, так и частных компаний. В отличие от США, в Китае регулирование

рассматриваемой сферы осуществляется централизованно. Однако и здесь долгое время (до ноября 2021 г.) не существовало специального закона, посвященного обработке персональных данных: вопрос регулировался главным образом правовыми актами в сфере безопасности. В 2016 г. был принят Закон «О кибербезопасности», глава IV которого посвящена вопросам сбора, обработки и защиты личных данных пользователей операторами сетей. В соответствии со ст. 31 Закона коммуникационные и информационные услуги, финансовая сфера и «электронное правительство» образуют критически важную информационную инфраструктуру государства, нарушение безопасности которой может поставить под угрозу национальную безопасность, национальное благосостояние, общественные интересы. Поэтому китайский подход к вопросам организации киберпространства «отличается большей концентрированностью государства на вопросах кибербезопасности, чем это характерно для стран западной демократии» [19. Р. 4]. Это проявляется в том числе в принятии мер по борьбе с анонимностью и установлении обязанности всех пользователей раскрывать свою подлинную личность при использовании глобальной Сети. Данный императив получил отражение и в регулировании сбора и последующей обработки биометрических данных интернет-пользователей.

Статья 76 Закона «О кибербезопасности» понимает под «личной информацией» «все виды информации, записанные в электронном виде или с помощью других средств, взятые отдельно или вместе с другой информацией, достаточные для идентификации личности физического лица, включая, помимо прочего, полные имена, даты рождения, национальные идентификационные номера, биометрические данные, информацию о месте жительства, номере телефона и т.д.». Признавая биометрические данные разновидностью личной информации, Закон не предусматривает специального режима их защиты и предоставляет операторам широкие возможности самостоятельно определять правила обработки личной информации, закрепляемые в собственных политиках обработки личной информации.

В 2021 г. в Китае вступили в силу сразу два закона – 1 сентября и 1 ноября соответственно: «О безопасности данных» и «О защите персональных данных». Раздел II последнего посвящен особенностям обработки «чувствительных» данных, к которым, помимо прочего, относится и биометрическая информация. Большинство норм этого раздела отсылают к другим законам и содержат лишь рамочное регулирование. В частности, ст. 29 Закона требует получения от субъекта данных отдельного согласия на сбор «чувствительной» информации, а ст. 30 обязывает операторов уведомлять субъектов о целях сбора информации и о том, какое влияние сбор такой информации может оказать на их права и интересы (Закон предусматривает в ст. 18, что нормативными правовыми актами могут предусматриваться исключения из этого правила). Отдельно регулируется порядок сбора персональных данных операторами интернет-

платформ со значительным числом пользователей. Они должны создавать системы контроля защиты данных в соответствии с установленными государственными требованиями, принимать правила платформ в соответствии с принципами прозрачности, ясности и справедливости, регулярно публиковать отчеты о деятельности в области защиты персональных данных и т.д.

Ни один нормативный акт не регулирует детально порядок передачи личной информации о пользователях операторами органам государства. Лишь Закон «О безопасности данных» 2021 г. в ст. 38 указывает, что государственные органы, собирающие или использующие данные для реализации своих полномочий, должны действовать исключительно в рамках, предписанных правовыми актами, и сохранять конфиденциальность персональных данных и личной информации. Закон «О защите персональных данных» также предусматривает некоторые правила, в частности обязанность органов государства уведомлять субъектов об обработке их данных. В то же время такое уведомление не требуется, если оно, например, будет «препятствовать органу власти осуществлять возложенные на него законом полномочия» (ст. 35). Расплывчатость подобных формулировок создает для государства фактически безграничные возможности по сбору и обработке личной информации, касающейся физических лиц, в том числе их биометрических персональных данных, и использовать их для целей биометрической идентификации.

В 2017 г. неправительственная организация *Human Rights Watch* обвинила китайскую компанию *iFlytek* в формировании для правительства НКНР базы данных образцов голосов граждан страны⁴. Несмотря на то, что никакого официального подтверждения этих подозрений представлено не было, логика законодательства Китая не исключает возможности обращения государственных органов к частным организациям, в том числе операторам интернет-платформ, за содействием при формировании биометрических баз, причем без ведома субъектов, к которым относится эта информация. Таким образом, концепция правового регулирования обработки биометрических данных в онлайн-пространстве построена на сочетании двух начал: с одной стороны, формирование высоких стандартов обработки биометрических данных частными организациями, с другой – предоставление фактически неограниченных возможностей их использования государством в национальных интересах. Несмотря на то, что принятые в 2021 г. законодательные акты во многом воспроизводят положения, присутствующие, в частности, в Общем регламенте Европейского союза по защите персональных данных, названная концепция осталась неизменной: частные интересы в ней во многом подчинены публичным интересам, реализуемым государством и его органами.

В рамках данной концепции осуществляется формирование государственной биометрической базы, причем активную роль в этом также играют частные компании – провайдеры интернет-услуг. Самым популярным приложением среди населения Китая явля-

ется *WeChat*, его используют 78% населения страны. *WeChat* представляет собой виртуальное пространство, в котором пользователи могут искать и получать информацию, общаться, играть, осуществлять финансовые транзакции и получать государственные услуги, в том числе доступ к правосудию. Использование многих функций приложения (в том числе в сфере финансов и госуслуг) требует идентификации субъекта с помощью сканирования геометрии его лица. В ряде регионов страны данное приложение используется и в качестве электронного удостоверения личности (в скором времени, вероятно, данная функция будет реализована на всей территории НКНР). В результате в Китае создается единая биометрическая база данных, контролируемая государством, но используемая для осуществления идентификации клиентов финансовыми и другими частными компаниями. Существующие в Китае государственные требования устанавливают, что при использовании программ распознавания лиц биометрические данные должны храниться отдельно от других идентификационных данных субъектов. Вместе с тем практически не ограниченный законом доступ государства к таким сведениям, обрабатываемым частными операторами, во многом ставит под сомнение существование в данной стране неприкосновенности частной жизни.

Европейский союз. В странах Европейского союза (ЕС) реализована еще одна модель правового регулирования биометрической идентификации. В отличие от Китая, где во главу угла поставлены вопросы обеспечения безопасности, в ЕС на первый план выходит обеспечение неприкосновенности частной жизни субъектов и обеспечения конфиденциальности их личных данных. Как и в США, правовое регулирование порядка обработки персональных данных (в том числе биометрических) осуществляется в ЕС на двух уровнях, однако законодательство верхнего (наднационального) уровня отличается от федерального законодательства США тем, что является кодифицированным. Оно представлено главным образом Общим регламентом по защите персональных данных (*General Data Protection Regulation – GDPR*, далее также Регламент). На уровне отдельных стран также существует национальное законодательство, но оно не должно противоречить Регламенту. В статье 4 GDPR биометрические данные определяются как «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».

Регламентом устанавливается специальный режим обработки биометрических данных, предполагающий общий запрет на совершение с ними каких-либо действий, кроме случаев, когда такая обработка прямо допускается. Среди оснований обработки биометрических данных названы явное согласие субъекта данных в рамках одной или нескольких определенных целей, исполнение обязанностей контролера в сфере

трудового законодательства, социального обеспечения и социальной защиты субъекта данных, защита жизненно важных интересов субъекта в случаях, когда сам субъект не в состоянии (физически или юридически) высказать свое явное согласие, обработка данных, которые субъект явным образом сделал публичными, обработка в рамках осуществления правосудия, важного публичного интереса и т.д. Этот перечень не является закрытым: государства – члены Европейского союза могут в своих законодательных актах предусмотреть и иные случаи обработки биометрических данных.

Применительно к онлайн-пространству наибольший интерес представляют два основания обработки биометрических данных: согласие субъекта персональных данных и размещение таких данных самим субъектом публично. Концепция согласия в соответствии с GDPR значительно отличается от тех, которые применяются в Соединенных Штатах Америки или в Китае и предполагает соблюдение не только принципов информированности и явности его выражения, но также принципов свободы и конкретности. В соответствии с Методическими рекомендациями Европейского Совета по защите персональных данных согласие необходимо рассматривать как «свободное» только в случае, если субъекту представляется реальная возможность:

- отказаться от дачи согласия, не испытывая страха несения негативных последствий;
- отозвать согласие, при этом процедура отзыва должна быть такой же простой, как и предоставления согласия.

Если согласие дается во исполнение договора, оно не должно являться неизменным условием такого договора, исполнение которого не может быть связано с наличием или отсутствием согласия. Кроме того, субъект персональных данных не должен находиться в социальной или экономической зависимости от контролера персональных данных.

Важным требованием к согласию на обработку биометрических данных (как и других «чувствительных» персональных данных) является его конкретность. В соответствии со ст. 9 Регламента согласие быть явным по отношению к одной или нескольким целям обработки. Субъекту данных должна быть предоставлена возможность высказать согласие или отказаться от его предоставления в отношении каждой из целей в отдельности, а сама формулировка цели обработки должна быть сформулирована предельно четко. Требование конкретности препятствует созданию единых баз биометрических данных, доступ к которой могли бы получать различные юридические лица при оказании услуг клиенту, как это практикуется в Китае, а с недавнего времени и в России.

Публичное размещение субъектом информации о себе в сети Интернет в ЕС не рассматривается в качестве достаточного основания для обработки биометрических данных. Пользователь может разместить в социальной сети свое изображение, аудиозапись голоса или фотографию своей руки, однако данные электронные записи не рассматриваются в качестве био-

метрических данных, поскольку таковые – как следует из приведенного выше определения – могут быть получены только в результате специальной технической обработки. В то же время извлечение биометрических данных из указанной личной информации, размещенной в интернете, может осуществляться при наличии иных оснований, предусмотренных ст. 9 Регламента. Применительно к поставщикам интернет-услуг в большинстве случаев единственным основанием для этого остается согласие субъекта данных.

С учетом существующего регулирования поставщики интернет-услуг, зарегистрированные в ЕС, значительно реже прибегают к обработке биометрических данных, нежели компании, зарегистрированные в Соединенных Штатах Америки или в некоторых странах Азии.

Российская Федерация. Регулирование обработки биометрических данных в Российской Федерации в настоящее время в большей степени тяготеет к модели, выбранной Китаем и рядом других стран Азии (Сингапуром, Индией, Турцией и др.). В основе регулирования лежит ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), согласно которой биометрическими персональными данными признаются сведения, которые, во-первых, характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и, во-вторых, используются оператором персональных данных для установления личности субъекта⁵. Важно отметить, что действие указанного Закона распространяется на обработку не любых сведений, относящихся к физиологическим и биологическим характеристикам индивида, а именно тех, которые используются для его идентификации [10. С. 87; 20. С. 253].

Часть 1 ст. 11 Закона о персональных данных устанавливает правило, согласно которому обработка биометрических данных возможна только с согласия субъекта. Вместе с тем в ч. 2 содержится ряд исключений. Не требуется получать согласие в следующих случаях:

- в связи с реализацией международных договоров Российской Федерации о реадмиссии;
- при осуществлении правосудия и исполнении судебных актов;
- в связи с проведением обязательной государственной дактилоскопической регистрации;
- если обработка биометрических данных предусмотрена законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-разыскной деятельности, о государственной службе; уголовно-исполнительным законодательством, законодательством о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве, а также о нотариате.

Таким образом, в России биометрическая идентификация субъектов может осуществляться без их согласия только в публично-правовых отношениях и

если это специально предусмотрено федеральным законом [20. С. 262]. В иных ситуациях (в том числе в частноправовых отношениях, включая идентификацию пользователей интернет-сервисов) получение согласия является обязательным условием. В отличие от США, где регулирование обработки биометрических данных допускается как на федеральном уровне, так и на уровне штатов, в России регулирование прав человека, информационных технологий, а также обеспечение безопасности личности при обороте цифровых данных относятся к сфере исключительно федерального ведения (п. «в», «и», «м» ст. 71 Конституции РФ).

С 29 декабря 2020 г. к числу оснований обработки биометрических данных без согласия субъекта добавилось установление личности гражданина, обратившегося за совершением нотариальных действий, в соответствии с законодательством РФ о нотариате (федеральные законы от 27 декабря 2019 г. № 480-ФЗ и от 30 декабря 2020 г. № 537-ФЗ). Данное нововведение связано с созданием в России единой биометрической системы и открытия к ней доступа нотариусов с целью биометрической идентификации граждан.

Федеральным законом от 31 декабря 2017 г. № 482-ФЗ в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) была введена ст. 14.1, регулирующая использование информационных технологий в целях идентификации граждан Российской Федерации, в том числе на основе биометрических персональных данных. Именно в ней был законодательно установлен правовой режим единой биометрической системы (ЕБС) – централизованной государственной базы данных, содержащей биометрические контрольные шаблоны, предназначенные для идентификации граждан без их личного присутствия. В связи с изменениями, внесенными в Закон об информации Федеральным законом от 29 декабря 2020 г. № 479-ФЗ, установленные в нем требования были распространены на идентификацию любых физических лиц, а не только граждан РФ. Создание ЕБС было анонсировано Минкомсвязи России еще в 2016 г., и в последующие годы проходила последовательная подготовка законодательной почвы для реализации этой инициативы.

Отбор биометрических данных для их внесения в ЕБС допускается только государственными органами, банками и другими организациями в случаях, когда это предусмотрено федеральными законами; с согласия лица и при его личном присутствии. В последующем обращение к ЕБС для аутентификации лица (путем сопоставления его биометрических данных с хранящимся в системе контрольным шаблоном) может осуществляться и иными организациями и индивидуальными предпринимателями, а также нотариусами. При этом Закон содержит следующие требования:

– лицо должно выразить согласие на проведение его аутентификации путем обращения к ЕБС (за исключением проведения аутентификации нотариусами);

– организации и индивидуальные предприниматели, использующие ЕБС для аутентификации физических лиц, должны отвечать установленным в п. 18.8 ст. 14.1 Закона об информации критериям, целью которых является пресечение мошеннических и иных недобросовестных действий с использованием биометрической информации. В частности, данные субъекты, а также члены органов управления организаций не должны быть причастны к терроризму или экстремизму; у индивидуального предпринимателя или у единоличного исполнительного органа организации не должно быть неснятой или непогашенной судимости, а в отношении организации в Едином государственном реестре юридических лиц не должно содержаться записи о недостоверности адреса.

Наряду с ЕБС (которая с 30 декабря 2021 г. приобретает статус государственной информационной системы) Закон об информации разрешает использовать для сбора, хранения и иной обработки биометрических данных также частные информационные системы. До начала использования соответствующие информационные технологии и технические средства должны получить подтверждение соответствия требованиям, которые устанавливаются Министерством цифрового развития, связи и массовых коммуникаций РФ (Минцифры России). Обновленные требования, а также порядок обработки биометрических персональных данных (в части изображений лиц и голосов) утверждены приказом Минцифры России от 10 сентября 2021 г. № 930 и вступят в силу с 1 марта 2022 г. (до этого времени применяется приказ Минкомсвязи России от 25 июня 2018 г. № 321).

Анализ практики правового регулирования биометрической идентификации и обработки биометрических данных в рассмотренных странах позволяет сделать вывод о формировании трех основных моделей. В основе каждой из них лежит определенная конституционно-правовая концепция установления баланса между интересами личности в сохранении неприкосновенности частной жизни и публичными интересами.

Первая концепция, воплощенная в американской модели правового регулирования, основана на идее свободы субъектов в распоряжении своими биометрическими данными. Государство исходит из необходимости саморегулирования в сфере биометрической идентификации и обработки личной информации, оставляя широкий простор для установления правил и процедур в пользовательских соглашениях и политиках, принимаемых провайдерами интернет-услуг, и обеспечивая лишь минимально необходимые законодательные гарантии соблюдения прав гражданина – главным образом в тех сферах, где субъекты являются наименее защищенными (финансовые услуги, отношения с участием несовершеннолетних и т.д.).

Вторая концепция получила развитие в модели, которая была описана на примере Китая и которую можно назвать «азиатской» (поскольку она характерна для многих других стран этого региона – Турции, Объединенных Арабских Эмиратов, Сингапура, Бахрейна, Пакистана, Бангладеш, а также начинает ак-

тивно применяться в африканских странах – Нигерии, Уганде, Танзании и в ряде стран Латинской Америки). Данная концепция поощряет развитие биометрической идентификации – причем как в онлайн-пространстве, так и в офлайн-среде. С этой целью государство строит регулирование таким образом, чтобы планомерно собирать данные о пользователях с частных провайдеров интернет-услуг и операторов связи и формировать централизованные базы биометрической информации для их использования в целях удаленной идентификации субъектов – как в государственных интересах или при предоставлении публичных услуг, так и при обращении субъектов к негосударственным операторам, имеющим доступ к таким базам. Пользовательские соглашения и политики, принимаемые операторами обработки данных в интернет-пространстве, должны соответствовать жестким государственным стандартам. Публичные интересы, заключающиеся, в частности, в обеспечении национальной безопасности, в этом случае превалируют над частными интересами отдельных субъектов в сохранении конфиденциальности своих данных.

Третья концепция лежит в основе европейской модели регулирования. Она признает необходимость детального регулирования обработки биометрической информации, однако, в отличие от предыдущей концепции, нацелена на защиту интересов субъектов в сохранении неприкосновенности частной жизни. Возможность обработки биометрической информации в интернете практически всегда зависит от явно выраженной воли субъекта данных и сопряжена с довольно жесткими требованиями к деятельности операторов и контролеров данных. Кроме того, концепция фактически отрицает идею единой базы биометрических данных для обеспечения идентификации пользователей в онлайн-пространстве, в том числе в связи с тем, что создание подобных централизованных баз не может обеспечить достаточного уровня безопасности данных о пользователях. Риски нарушения приватности в случае утечки данных рассматриваются в данном случае как неоправданные.

Законодательное регулирование оборота биометрической информации в России в большей степени основано на второй концепции и развивается в рамках модели, характерной для азиатских стран. «Азиатская» модель правового регулирования, вероятно, в большей степени (в сравнении с двумя другими моделями) способствует максимально широкому внедрению технологий биометрической идентификации в онлайн-среду. За счет применения «сквозных» технологий, допускающих биометрическую идентификацию личности как в интернете, так и в физической реальности, стирается граница между виртуальным и физическим мирами. «Виртуальная личность» интернет-пользователя при этом все больше становится не просто цифровым отражением или аватаром «физического» субъекта, а его частью и юридическим продолжением.

По этой причине возрастают и риски. Первый из них заключается в серьезном ограничении приватно-

сти субъектов, их права на сохранение тайны частной жизни в результате фактической утраты контроля за обрабатываемыми биометрическими данными. Второй (возможно, даже еще более значимый) – риск злоупотреблений, в том числе в случае утечки данных из биометрических баз. Как показывает практика, в России случаи утечки персональных данных из государственных баз, увы, не являются редкостью [20. С. 260–261], а неправомерный доступ к биометрическим данным – ввиду наличия у них таких свойств, как неизменяемость и неотчуждаемость от субъекта-носителя – способен повлечь негативные последствия, исправить которые будет крайне сложно. Риски введения в России ЕБС уже отмечались отечественными учеными [7. С. 113; 21].

Главной проблемой по-прежнему остается недостаточное качество правового регулирования получения согласий субъектов на обработку биометрических персональных данных (в том числе извлекаемых в автоматизированном режиме из размещенных в интернете изображений), допускающее получение таких согласий в упрощенной форме (например, путем выражения пользователем согласия с политикой конфиденциальности интернет-сервиса). Цели сбора и обработки биометрической информации часто прописываются в таких политиках общими фразами, без должной конкретизации (например, «для улучшения работы сервиса»), что допускает практически безграничное использование персональных данных операторами и фактически лишает субъектов возможности контролировать дальнейший оборот предоставленных данных. Существуют и проблемы, связанные с установлением требований к технологиям обработки биометрических персональных данных владельцами интернет-сервисов, в том числе при предоставлении государственных услуг. Имеющиеся технические требования не в полной мере защищают данные о пользователях от возможных утечек. В частности, следовало бы на уровне федерального закона установить в качестве гарантии прав личности требование раздельного хранения биометрических идентификаторов (причем обязательно в зашифрованном виде) и данных о лице, которому такие идентификаторы принадлежат. Наконец, ответственность операторов и их должностных лиц за нарушения порядка обработки персональных данных, предусмотренная, в частности, ст. 13.11 Кодекса РФ об административных правонарушениях, также является весьма мягкой в сравнении с мерами, существующими, например, в Китае или в ряде европейских стран. Названные проблемы, существующие в России, делают человека уязвимым перед лицом технологий обработки биометрической информации в онлайн-среде.

В отличие от Китая и других азиатских стран, а также стран Африки и Латинской Америки, Россия является членом Совета Европы, международные документы которого задают высокие стандарты в области прав человека, в том числе прав, связанных с неприкосновенностью частной жизни. По этой причине регулирование обработки биометрической информации и порядка биометрической идентификации в интернете, вводимое в

нашей стране, должно учитывать не только позитивный опыт Китая или Сингапура в части технических реше-

ний, но и принятые Россией международные обязательства по защите прав личности.

Примечания

¹ Статистические данные приведены по данным сайта: <https://www.statista.com/statistics/617136/digital-population-worldwide> (дата обращения: 01.11.2021).

² Как в теории, так и на практике процедуры идентификации и аутентификации, как правило, различают, понимая под «идентификацией» процесс первичного установления личности субъекта и создания идентификатора, а под «аутентификацией» - проверку подлинности личности субъекта путем удостоверения принадлежности ему соответствующего идентификатора. Для целей настоящей статьи мы будем использовать термин «идентификация» в широком значении как любой процесс установления, подтверждения или проверки подлинности личности субъекта на основе биометрических данных, включающий в себя не только первичную идентификацию, но и последующие акты аутентификации.

³ Официальное наименование законопроекта S.4400 – National Biometric Information Privacy Act of 2020. Прохождение законопроекта можно отследить на сайте Конгресса США: <https://www.congress.gov/bill/116th-congress/senate-bill/4400> (дата обращения: 01.11.2021).

⁴ China: Voice Biometric Collection Threatens Privacy. URL: <https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy> (дата обращения: 01.11.2021).

⁵ Положения нормативных правовых актов Российской Федерации приведены по состоянию на 1 ноября 2021 г. При подготовке статьи использована справочно-правовая система «КонсультантПлюс».

Список источников

1. Laptev V., Fedin V. Legal Awareness in a Digital Society // Russian Law Journal. 2020. Vol. 8, № 1. P. 138–157. doi: 10.17589/2309-8678-2020-8-1-138-157
2. Bertillon A. Identification anthropométrique: instructions signalétiques. Melun: Imprimerie Administrative, 1893. 148 p.
3. Gomez-Barrero M., Drozdowski P., Rathgeb C. et al. Biometrics in the Era of COVID-19: Challenges and Opportunities (February 2021). URL: <https://arxiv.org/pdf/2102.09258.pdf> (дата обращения: 01.11.2021).
4. Григорьев В.Н. Информационные технологии в расследовании массовых беспорядков // Вестник Санкт-Петербургского университета. Право. 2021. № 2. С. 334–355. doi: 10.21638/spbu14.2021.206
5. Ang K.L., Seng K.P. Biometrics-based Internet of Things and Big data design framework // Mathematical Biosciences and Engineering. 2021. Vol. 18, № 4. P. 4461–4476. doi: 10.3934/mbe.2021226
6. Daly M.P., Deal K., Duffy S.C. et. al. Biometrics Litigation: An Evolving Landscape (Practical Law Litigation, April – May 2016). URL: [https://uk.practicallaw.thomsonreuters.com/w-001-8264?_lrTS=20170720182117024&transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-001-8264?_lrTS=20170720182117024&transitionType=Default&contextData=(sc.Default)&firstPage=true) (дата обращения: 01.11.2021).
7. Рассолов И.М., Чубукова С.Г., Микурова И.В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica (Русский закон). 2019. № 1. С. 108–118.
8. Huang J. Applicable Law to Transnational Personal Data: Trends and Dynamics // German Law Journal. 2020. Vol. 21. № 6. P. 1283–1308. doi:10.1017/glj.2020.73
9. Платонова Н.И. Современные правовые подходы к пониманию биометрических данных // Информационное право. 2018. № 1. С. 22–27.
10. Кривогиин М.С. Особенности правового регулирования биометрических персональных данных // Право. Журнал Высшей школы экономики. 2017. № 2. С. 80–89.
11. Nguyen F.Q. The Standard for Biometric Data Protection // Journal of Law & Cyber Warfare. 2018. Vol. 7, № 1. P. 61–84.
12. Voss W., Houser K. Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies // American Business Law Journal. 2019. Vol. 56, Is. 2. P. 287–344. doi: 10.1111/ablj.12139
13. Benson B. Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy // North Carolina Journal of Law & Technology. 2018. Vol. 19, Is. 4. P. 161–192.
14. Zimmerman H. The Data of You: Regulating Private Industry's Collection of Biometric Information // Kansas Law Review. 2018. Vol. 66, Is. 3. P. 637–671.
15. Bock M.E. Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act // North Carolina Banking Institute. 2020. Vol. 24, Is. 1. P. 309–330.
16. Illman E.J. Data Privacy Laws Targeting Biometric and Geolocation Technologies // The Business Lawyer. 2018. Vol. 73, № 1. P. 191–197.
17. Rivera M.A. Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies // Fordham Intellectual Property, Media and Entertainment Law Journal. 2019. Vol. 29, № 2. P. 571–610.
18. Ropiequet J.L., Doss A.F., Pennacchio V.G. The Next Big Thing: Current Issue Under the Illinois Biometric Information Privacy Act // Quarterly Report. 2020. Vol. 74, № 1. P. 43–69.
19. Swaine M.D. Chinese Views on Cybersecurity in Foreign Relations // China Leadership Monitor. 2013. № 42. P. 4.
20. Савельев А.И. Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд. М.: Статут, 2021. 468 с.
21. Матюхина Е.Н. Российское и германское законодательство о персональных данных: сравнительный анализ подходов и практики применения // Lex russica (Русский закон). 2019. № 4. С. 170–178. doi: 10.17803/1729-5920.2019.149.4.170-178

References

1. Laptev, V. & Fedin, V. (2020) Legal Awareness in a Digital Society. *Russian Law Journal*. 1 (8). pp. 138–157. DOI: 10.17589/2309-8678-2020-8-1-138-157
2. Bertillon, A. (1893) *Identification anthropométrique: instructions signalétiques*. Melun: Imprimerie Administrative.
3. Gomez-Barrero, M. et al. (2021) *Biometrics in the Era of COVID-19: Challenges and Opportunities*. [Online] Available from: <https://arxiv.org/pdf/2102.09258.pdf> (Accessed: 01.11.2021).
4. Grigor'ev, V.N. (2021) Information technology in the investigation of riots. *Vestnik Sankt-Peterburgskogo universiteta. Pravo – Vestnik of Saint Petersburg University. Law*. 2 (12). pp. 334–355. (In Russian). DOI: 10.21638/spbu14.2021.206
5. Ang, K.L. & Seng, K.P. (2021) Biometrics-based Internet of Things and Big data design framework. *Mathematical Biosciences and Engineering*. 4 (18). pp. 4461–4476. DOI: 10.3934/mbe.2021226
6. Daly, M.P. et al. (2016) Biometrics Litigation: An Evolving Landscape (Practical Law Litigation, April – May 2016). *Practical Law*. [Online] Available from: [https://uk.practicallaw.thomsonreuters.com/w-001-8264?_lrTS=20170720182117024&transitionType=Default&contextData=\(sc.Default\)&firstPage=true](https://uk.practicallaw.thomsonreuters.com/w-001-8264?_lrTS=20170720182117024&transitionType=Default&contextData=(sc.Default)&firstPage=true) (Accessed: 01.11.2021).

7. Rassolov, I.M., Chubukova, S.G. & Mikurova, I.V. (2019) Biometrics in the context of personal data and genetic information: legal issues. *Lex russica (Russkiy zakon)*. 1 (146). pp. 108–118. (In Russian). DOI: 10.17803/1729-5920.2019.146.1.108-118
8. Huang, J. (2020) Applicable Law to Transnational Personal Data: Trends and Dynamics. *German Law Journal*. 6 (21). pp. 1283–1308. DOI:10.1017/glj.2020.73
9. Platonova, N.I. (2018) Modern legal approaches to interpretation of biometric data. *Informatsionnoe pravo – Information Law*. 1. pp. 22–27. (In Russian).
10. Krivogin, M.S. (2017) Peculiarities of legal regulating biometric personal data. *Pravo. Zhurnal Vysshey shkoly ekonomiki – Law. Journal of the Higher School of Economics*. 2. pp. 80–89. (In Russian). DOI: 10.17323/2072-8166.2017.2.80.89
11. Nguyen, F.Q. (2018) The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*. 1 (7). pp. 61–84.
12. Voss, W. & Houser, K. (2019) Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. *American Business Law Journal*. 2 (56). pp. 287–344. DOI: 10.1111/ablj.12139
13. Benson, B. (2018) Fingerprint Not Recognized: Why the United States Needs to Protect Biometric Privacy. *North Carolina Journal of Law & Technology*. 4 (19). pp. 161–192.
14. Zimmerman, H. (2018) The Data of You: Regulating Private Industry's Collection of Biometric Information. *Kansas Law Review*. 3 (66). pp. 637–671.
15. Bock, M.E. (2020) Biometrics and Banking: Assessing the Adequacy of the Gramm-Leach-Bliley Act. *North Carolina Banking Institute*. 1 (24). pp. 309–330.
16. Illman, E.J. (2018) Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*. 1 (73). pp. 191–197.
17. Rivera, M.A. (2019) Face Off: An Examination of State Biometric Privacy Statutes & Data Harm Remedies. *Fordham Intellectual Property, Media and Entertainment Law Journal*. 2 (29). pp. 571–610.
18. Ropiequet, J.L., Doss, A.F. & Pennacchio, V.G. (2020) The Next Big Thing: Current Issue Under the Illinois Biometric Information Privacy Act. *Quarterly Report*. 1 (74). pp. 43–69.
19. Swaine, M.D. (2013) Chinese Views on Cybersecurity in Foreign Relations. *China Leadership Monitor*. 42. pp. 4.
20. Savel'ev, A.I. (2021) *Nauchno-prakticheskiy postateynnyy kommentariy k Federal'nomu zakonu "O personal'nykh dannykh"* [Scientific and practical article-by-article commentary on the Federal Law "On Personal Data"]. 2nd ed. Moscow: Statut.
21. Matyukhina, E.N. (2019) Russian and German legislation on personal data: comparative analysis of approaches and practices. *Lex russica (Russkiy zakon)*. 4 (149). pp. 170–178. (In Russian). DOI: 10.17803/1729-5920.2019.149.4.170-178

Информация об авторах:

Кузнецова С.С. – канд. юрид. наук, доцент кафедры конституционного права Уральского государственного юридического университета (г. Екатеринбург, Россия). E-mail: kss001@usla.ru.

Мочалов А.Н. – канд. юрид. наук, доцент кафедры конституционного права Уральского государственного юридического университета (г. Екатеринбург, Россия). E-mail: artur.mochalov@usla.ru.

Саликов М.С. – д-р юрид. наук, зав. кафедрой конституционного права Уральского государственного юридического университета (г. Екатеринбург, Россия). E-mail: kp@usla.ru.

Авторы заявляют об отсутствии конфликта интересов.

Information about the author:

S.S. Kuznetsova, Cand. Sci. (Law), associate professor, Ural State Law University (Yekaterinburg, Russian Federation). E-mail: kss001@usla.ru

A.N. Mochalov, Cand. Sci. (Law), associate professor, Ural State Law University (Yekaterinburg, Russian Federation). E-mail: artur.mochalov@usla.ru

M.S. Salikov, Dr. Sci. (Law), head of the Department of Constitutional Law, Ural State Law University (Yekaterinburg, Russian Federation). E-mail: kp@usla.ru

The authors declare no conflicts of interests.

Статья поступила в редакцию 20.12.2021;
одобрена после рецензирования 10.02.2022; принята к публикации 28.03.2022.

The article was submitted 20.12.2021;
approved after reviewing 10.02.2022; accepted for publication 28.03.2022.