УДК 342.72/.73

Морозов Роберт Алексеевич

аспирант кафедры конституционного права
Российский государственный университет правосудия
Москва, Россия

Robert A. Morozov

Postgraduate student of the Department of Constitutional Law
Russian State University of Justice
Moscow, Russia

БЕЗОПАСНОСТЬ БИОМЕТРИЧЕСКИХ ДАННЫХ ЛИЧНОСТИ ЧЕРЕЗ ПРИЗМУ ЦИФРОВИЗАЦИИ

SECURITY OF PERSONAL BIOMETRIC DATA THROUGH THE PRISM OF DIGITALIZATION

Аннотация

В эпоху цифровизации мы всё чаще пользуемся биометрическими данными – от разблокировки телефона до входа в систему государственных услуг. Однако наряду с преимуществами цифровизации возникает множество угроз, связанных с утечками и фальсификацией биометрических параметров. В статье рассмотрены особенности правового обеспечения безопасности биометрических данных в Российской Федерации, проанализированы риски и угрозы правам человека при использовании биометрической идентификации. В том числе, в рамках статьи изучена правовая регламентация деятельности цифровой биометрической платформы в России, изучены методы защиты биометрических данных.

Ключевые слова:

биометрические данные, права и свободы личности, биометрическая идентификация

Abstract

In the age of digitalization, we are increasingly using biometric data - from unlocking the phone to logging into the system of public services. However, along with the benefits of digitalization, there are many threats associated with leaks and falsification of biometric parameters. This article will consider the specifics of the legal provision of biometric data security in the Russian Federation, analyze the risks and threats to human rights when using biometric identification. In particular, the article will examine the legal regulation of the digital biometric platform in Russia, and methods of protecting biometric data.

Keywords:

biometric data, personal rights and liberties, biometric identification

Обеспечение безопасности – ключевой аспект процесса цифровизации, особенно если речь идет об одном из видов персональных данных – биометрических данных. В рамках цифровизации многочисленных государственных процессов, например, государственных услуг, большинство операций совершается путем использования различных способов верификации (подтверждения) личности.

Применение биометрических данных для идентификации человека порождает множество потенциальных рисков для защиты прав и свобод граждан. В связи с чем, значимость и необходимость защиты биометрических данных, в контексте права на защиту персональных данных, ставит вопрос их регулирования на уровень конституционно-правового; от степени защищенности биометрических данных напрямую зависит реализация основополагающих конституционных прав человека [3, С. 259].

Биометрические данные личности – это уникальные биологические характеристики, используемые для идентификации и аутентификации личности. Зарубежные исследователи придерживаются мнения, что биометрические данные не только представляют собой информацию о человеке, но и выступают способом обеспечения уникальной связи данной информации с конкретным лицом и, следовательно, могут служить идентификатором определенного лица [5, С. 302].

К биометрической информации, по мнению И. Л. Бачило, относятся отпечатки пальцев, зрачки глаз человека, его ДНК и другие элементы индивида, широко используемые в практике идентификации субъекта [1, С.138]. В том числе, к биометрическим данным относится голос, геометрические особенности лица человека, узоры вен ладони [2, С.120].

В современном мире биометрические данные все чаще применяются в различных сферах, в том числе для получения государственных услуг, верификации в банковских организациях, доступа к устройствам и программам. Биометрическая идентификация в настоящее время существует как объективная необходимость подтверждения личности, иными словами, она необходима для отождествления пользователя устройства или пользователя в интернете с реальным субъектом права.

Несмотря на очевидные удобства применения, использование биометрических данных, как уже отмечалось, поднимает ряд серьезных вопросов, касающихся их защиты. В случае если украденный пароль можно заменить на миллионы иных комбинаций, то биометрические данные – это уникальный и неповторимый набор характеристик человека, который невозможно изменить также легко. Данная позиция подтверждается мнениями исследователей в этой сфере, согласно которым, биометрические параметры, непосредственно связанные со своим субъектом-носителем, остаются неизменными на протяжении всей жизни человека [4, С. 110].

Угрозы, связанные с использованием биометрических данных, позволяют определить их как самые «уязвимые данные», нуждающиеся в постоянной и эффективной защите [3, С. 258]. Именно поэтому во всем мире предпринимаются попытки обеспечить максимальную защиту, например, посредством раздельного хранения биометрических и иных персональных данных личности, сочетания при идентификации биометрии и пароля (кода).

Биометрические данные, как и персональные данные, могут быть украдены злоумышленниками посредством получения доступа к серверу, на котором хранится

информация. Сканирование отпечатков пальцев, фотографирование лица или запись голоса – все эти данные могут быть использованы для создания поддельных идентификаторов личности. В случае кражи параметров биометрии человека, что само по себе является серьезной угрозой для прав личности, дальнейшее использование этих данных для «надежной» идентификации себя невозможно, поскольку данные уже были скомпрометированы.

В настоящее время существует огромное количество устройств, которые имеют доступ к биометрическим данным граждан. Однако сбор этих данных не урегулирован нормативным актом, предусматривающим ответственность организации за возможное незаконное использование этих данных, а лишь регламентируется пользовательским соглашением и подтверждается добровольным согласием владельца устройства. Например, ежедневно миллионы пользователей «Iphone» предоставляют компании свои физиологические и биологические характеристики для доступа к телефону посредством отпечатков пальцев пользователя или изображения лица (его геометрических характеристик). Таким образом, «Face-ID» и иные биометрические данные могут храниться на иностранных серверах и, в последующем, могут быть использованы иностранными государствами против интересов граждан Российской Федерации.

Использование зарубежного программного обеспечения для идентификации личности также порождает многочисленные угрозы для биометрических данных. В связи с чем, в России уже длительное время ведется активный переход на отечественное программное обеспечение и на собственные, независимые и защищенные базы данных. В 2022 году был издан Федеральный закон «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» №572-ФЗ, в соответствии с которым была регламентирована деятельность Единой биометрической системы (ЕБС), которая, в свою очередь, стала цифровой биометрической платформой, аккумулирующей все биометрические данные в Российской Федерации. В результате, все биометрические данные были переданы в государственную информационную платформу ЕБС, а организации, которые фактически собирали эти данные, получили возможность за плату иметь доступ лишь

к математическим кодам, которые сами по себе не являются биометрическими данными человека. Данные в ГИС ЕБС хранятся на защищенных серверах в зашифрованном виде, в том числе, биометрические данные не хранятся едино с персональными данными личности, что, по сути, лишает их какой либо привлекательности для преступников, так как определить владельцев биометрических данных практически невозможно. Использование ЕБС не только позволяет обеспечить защиту биометрических данных на государственном уровне, в том числе посредством запрета на обработку биометрических данных иностранными организациями, но и повышает удобство ведения административной, криминалистической и судебной работы, получения различных услуг и использования государственных сервисов; предоставляет возможность подтверждать и совершать юридически значимые действия «онлайн». Несмотря на положительные аспекты, определенное количество уязвимых мест по-прежнему присутствует и по сегодняшний день. Современные технологии позволяют использовать для имитации чужой биометрии искусственно созданные лица и голоса, сгенерированные нейронными сетями или искусственным интеллектом, например «Liveness» или Deepfake», с целью получения доступа к документам или банковским средствам.

В результате глобальной цифровизации биометрические данные личности, в итоге, будут использоваться повсеместно. Однако будут ли они находится в безопасности – зависит от оптимальности правового режима их защиты и технической обеспеченности биометрических систем. На текущем этапе в России предпринимаются действия по эффективному управлению системами обработки данных, регулируется деятельность операторов биометрических данных, совершенствуются способы шифрования и хранения данных – все эти меры обеспечивают реализацию прав человека и их прямую защиту от посягательств.

В свою очередь, негативным аспектом является тот факт, что в настоящее время в России отсутствуют специализированные нормативные акты, регламентирующие использование биометрических технологий, выходящих за рамки применения Единой биометрической системы, что создает так называемую «серую зону» в правовом пространстве и может негативно сказаться на безопасности использования биометрических данных.

Таким образом, безопасность биометрических данных личности – это неотъемлемая часть их широкого применения. Только комплексный подход,

включающий технологические и законодательные аспекты, позволит обеспечить эффективную защиту биометрических данных от несанкционированного доступа и злоупотреблений.

Список использованных источников

1. Бачило И. Л. Информационное право: учебник для магистров. 3-е изд., перераб. и доп. М.: Юрайт, 2013. 576 с.

2. Карпушина А.В. К понятию биометрических персональных данных // Вестник Белгородского юридического института МВД России имени И.Д. Путилина. – 2023. – № 4. – С. 118-123.

3. 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.

4. 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.

5. Krausová A., Hazan H., Matejka J. Biometric Data Vulnerabilities: Privacy Implications // The lawyer quarterly. 2018. No. 3. pp. 295-305.