УДК 342.7

Защита персональных данных в виртуальной и дополненной реальности: правовой аспект

Александрова А.С.
Магистрант Юридического института
Самарского национального исследовательского
университета имени академика С.П. Королева

Цель статьи – формирование подходов к правовому регулированию обработки персональных данных в условиях распространения технологий виртуальной и дополненной реальности (VR/AR). Автор указывает на повышенный интерес и быстро растущую в обществе популярность технологий виртуальной и дополненной реальности, которые позволяют получить реалистичные впечатления, стирающие грани между физическим и цифровым мирами. Вследствие быстрой интеграции этих технологий в повседневную жизнь возникают весьма сложные вопросы, связанные с защитой персональных данных пользователей. Необходимость повышения уровня защиты персональных данных в условиях распространения технологий виртуальной и дополненной реальности в ближайшем будущем поставит новые задачи в сферах правотворчества и правоприменения.

Актуальность исследования заключается в том, что при использовании технологий VR/AR безопасность персональных данных пользователей может подвергаться серьезным рискам. Автором обоснована необходимость расширения возможностей пользователей по управлению персональными данными при использовании устройств VR/AR, а также целесообразность принятия государством упреждающих мер для защиты персональных данных своих граждан. Автором произведен анализ и сравнение видов персональных данных лиц, использующих технологии VR/AR, а также степень роста угроз конфиденциальности в случае возможной утечки информации. Также была проанализирована существующая в Российской Федерации нормативная основа обеспечения защиты персональных данных и выявлена необходимость реализации дальнейших правовых инициатив в этой сфере.

Предложен комплекс мер, направленных на обеспечение неприкосновенности частной жизни пользователей технологий виртуальной и дополненной реальности.

Ключевые слова: правовое регулирование, информационные технологии, персональные данные, конфиденциальность, виртуальная реальность, дополненная реальность, неприкосновенность частной жизни

Виртуальная реальность (*VR, virtual reality*) и дополненная реальность (*AR, augmented reality*) являются весьма актуальными цифровыми технологиями в настоящее время. С их развитием связываются перспективы цифровизации многочисленных сторон общественной и частной жизни. Технологии виртуальной и дополненной реальности сходны в том, что с их помощью человек помещается в искусственную обстановку, заменяющую или дополняющую действительность. Помимо общих черт у *VR* и *AR* есть и отличия, в основном состоящие в специфике их технической реализации.

Суть виртуальной реальности заключается в том, что при помощи технических средств происходит воспроизведение обстановки, имитирующей реальный мир. Помимо визуализации реального мира,

действия в виртуальной реальности могут осуществляться с применением имитации соответствующих физических действий, например, езды на автомобиле, катания на американских горках, плавания на лодке, прыжка с парашютом и многого другого. Для погружения в виртуальную реальность используется специальное оборудование – очки или шлемы, с помощью которых виртуальному миру придается максимально возможная на сегодня реалистичность. С помощью технологий дополненной реальности (*AR*) происходит наложение цифрового изображения на объекты реального мира путем использования определенных компонентов, таких как звуковые эффекты, сенсоры, визуальное восприятие [1].

Виртуальная и дополненная реальность схожи тем, что предоставляют человеку возможность воспринять как реальность вещи, существующие исключительно в цифровой форме. Отличает же их следующее – с помощью технологий виртуальной реальности создается совершенно новый мир, отчужденный от действительности, в то время как дополненная реальность добавляет некоторые цифровые элементы в реальный мир.

Развитие перечисленных технологий в ближайшей перспективе может осложнить реализацию гарантий неприкосновенности частной жизни и защиты персональных данных. Правовая основа обработки персональных данных, созданная в Российской Федерации, в целом обеспечивает необходимый уровень их защиты. Однако уникальный характер технологий виртуальной и дополненной реальности может потребовать законодательных новаций и регуляторных инициатив.

Основным правовым актом, регулирующим защиту персональных данных в Российской Федерации, является Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных», принятый в 2006 г. (далее – Закон о персональных данных). В соответствии с ключевыми положениями Закона, операторы обязаны получать согласие субъектов на обработку их персональных данных, принимать меры для защиты персональных данных от несанкционированного доступа или разглашения, а также предоставлять субъектам доступ к их персональным данным [2].

Применение Закона о персональных данных в условиях широкого распространения технологий виртуальной и дополненной реальности – сложный процесс. С одной стороны, персональные данные по определению включают в себя информацию, относящуюся прямо или косвенно к определенному или определяемому физическому лицу. Следовательно, и информация, собираемая с помощью *VR/AR*-технологий, также может быть отнесена к категории персональных данных.

С другой стороны, уникальные характеристики данных виртуальной/дополненной реальности, включая их иммерсивный и интерактивный характер, могут не в полной мере учитываться в правовом регулировании.

В отличие от действительности, в виртуальной реальности все данные о действиях и поведении людей могут храниться и подвергаться обработке в цифровой форме. Все происходящее в виртуальной реальности регулируется оператором, который отвечает за сохранность информации и технически может распоряжаться ей так, как посчитает нужным. Следует также учитывать, что при использовании систем виртуальной реальности образуется объем данных, превышающий поток информации в традиционных интернет-коммуникациях. Виртуальная реальность позволяет людям выражать эмоции и испытывать ощущения, которые невозможно выразить при общении с помощью мессенджеров, электронных писем и обычных двухмерных вебстраниц. Поскольку виртуальная реальность ощущается практически как реальный мир, у пользователя может возникнуть иллюзия доверительного общения, которое невозможно в открытом общественном пространстве. В такой ситуации человек способен раскрыть тайны своей частной жизни, рассчитывая на полную конфиденциальность [3].

Органы публичной власти уже обеспокоены возможностью утраты контроля над цифровыми аспектами жизни граждан. Широкий резонанс получил призыв Президента Российской Федерации о защите аватаров граждан России в метавселенной: «Государство должно взять на себя ответственность за хранение критически важной информации. Речь уже идет не о том, чтобы обеспечить кибербезопасность самого человека, но и его виртуального двойника – аватара внутри формирующихся метавселенных» [4].

Поскольку люди могут действовать в виртуальной реальности в виде аватаров с персональными идентификаторами, обоснован вывод, что информация, составляющая виртуальную реальность, может содержать персональные данные. Данные человека, который находится в виртуальной или дополненной реальности, можно разделить на общие данные, по которым можно определить личность человека, и на связанные, по которым невозможно точно определить личность человека без общих данных [5].

Общие данные – это информация, непосредственно раскрывающая личность человека, использующего технологии виртуальной или дополненной реальности, которая может быть собрана, записана, накоплена, систематизирована, сохранена и т.д. К таким данным, как минимум, относится виртуальное изображение пользователя – аватар, представляющий собой графическое изображение, создаваемое на основе восприятия человеком самого себя в реальном мире, имеющего сходство с его телом, чертами лица, одеждой и даже манерой поведения.

Тем самым человек сам предоставляет данные о себе, что в большинстве случаев может привести к раскрытию его личности. Помимо графического представления могут также добавляться имя человека, его пол и возраст, то есть биографические данные, а также могут фиксироваться данные о времени, в течение которого человек использовал *VR/AR* устройства [6].

Значительное количество данных обрабатывается во время воспроизведения физического присутствия в *VR* или *AR*. Для этого необходима информация о биометрических данных, которые считываются со специальных устройств в режиме реального времени. К таким устройствам относятся:

– устройства, которые могут фиксировать и отслеживать отпечатки пальцев и движения рук;

– устройства, которые могут отслеживать движения сразу в трех направлениях (*3DoF*);

– устройства, отслеживающие движения всего тела (*6DoF*);

– устройства, отслеживающие движение зрачка и взгляда в целом;

– устройства, которые могут измерить активность деятельности мозга (технология *BCI*), чтобы отследить восприимчивость человека к тем или иным действиям.

Пока не представляется возможным сделать так, чтобы сведения о личности, создаваемые в результате пребывания в виртуальной или дополненной реальности, не считывались. Человеку свойственно генерировать поток данных в любой момент времени. Он производит движения руками и ногами, поворачивается, качает головой, издает звуки и т.д. Информация об этих событиях считывается автоматически, поэтому возникает риск обработки весьма чувствительной информации о человеке [7].

К связанным данным относится информация, которая не содержит описательных сведений о человеке (например, имя пользователя, логин, пароль, *PIN*-код, платежная информация, *IP*-адрес и т.д.). Как указывалось выше, связанные данные, в отличие от общих данных, сами по себе не могут быть использованы для получения информации о физиологических данных человека, но при этом они необходимы для идентификации и аутентификации в информационной системе. Полученные данные используются исключительно для взаимодействия пользователя с его учетными записями, паролями и аккаунтами.

В случае получения неправомерного доступа к связанным данным непосредственной угрозы для утечки информации о личности нет. Однако данные о действиях и предпочтениях личности в виртуальном мире могут быть использованы против нее в случае объединения с другой информацией о человеке. Чтобы избежать таких случаев, недостаточно введения специальных правовых норм, запрещающих объединять различную информацию о человеке, которая может навредить ему в случае ее утечки. Существующие социальные нормы, направленные на запрет объединения баз персональных данных, далеко не всегда соблюдаются, а их санкции в силу мягкости обычно не рассматриваются как серьезное препятствие для правонарушителей.

Поэтому баланс социальных и технических мер, направленных на защиту персональных данных, следует сместить в сторону технического регулирования. Выход видится в применении технических норм: оптимизации сбора персональных данных и предоставлении больших возможностей по управлению ими самим гражданам.

Следует минимизировать объем полученных данных. Полученные данные необходимо обрабатывать только на тех устройствах, надежность которых не вызывает сомнений, а также не допускать их передачу через информационно-телекоммуникационные сети. Также имеет смысл устанавливать различные уровни доступа к таким данным. Действуя подобным образом, можно повысить уровень защищенности персональных данных и снизить вероятность, что данные человека станут доступны третьим лицам без его согласия.

Расширение возможностей пользователей по управлению персональными данными при использовании устройств *VR/AR* означает необходимость реализации следующих мер:

1. Ознакомление в обязательном порядке с политикой конфиденциальности. Политика конфиденциальности представляет собой документ, в котором указывается, какие персональные данные собираются, для чего они нужны и каким способом обрабатываются. Ознакомление с политикой конфиденциальности должно стать необходимым условием при использовании технологий, предполагающих столь масштабный сбор личных данных [8].

2. Получение согласия на обработку персональных данных. Чтобы уменьшить риск утечки данных и обеспечить их максимальную сохранность, необходимо усовершенствовать форму согласия на обработку персональных данных для иммерсивных трехмерных систем. Форма получения согласия, насколько это возможно, должна быть интегрирована в информационную систему, обеспечивающую доступ к технологиям *AR/VR*.

3. Обязательное использование двухфакторной аутентификации. Суть двухфакторной аутентификации заключается в том, что проверка личности производится в два этапа. Сначала пользователю необходимо ввести свои логин и пароль, затем еще раз подтвердить право на доступ к информационной системе, введя уникальный код, полученный по смс-сообщению, электронной почте или с помощью специального ПО. Этот процесс является дополнительной гарантией безопасности и будет способствовать

повышению уровня защиты данных от несанкционированного доступа.

4. Регулярное и в некоторых случаях принудительное обновление программного обеспечения устройств. Цифровой мир и технологии очень быстро совершенствуются, добавляются новые функции и параметры, улучшающие работу устройств и упрощающие взаимодействие с ними, поэтому важно следить за выходом новых обновлений и регулярно вносить изменения в устройства виртуальной и дополненной реальности. Поэтому для обновления программного обеспечения, имеющего критическую важность для защиты данных в системах *AR/VR*, допустима установка ПО без согласия пользователя. Однако информация о принципиальной возможности такого обновления должна быть однозначно и недвусмысленно доведена до сведения пользователей до начала эксплуатации информационной системы.

Применяя вышеуказанные способы защиты информации, можно обеспечить сохранность персональных данных, сведя к минимуму возможность утечки конфиденциальных сведений.

По мере развития технологий виртуальной/дополненной реальности и их интеграции в повседневную жизнь потребность в эффективной защите персональных данных будет расти. Поэтому необходимо постоянное взаимодействие законодателей, органов исполнительной власти, производителей устройств, а также объединений потребителей для обеспечения соответствия нормативного регулирования защиты персональных данных уровню развития информационных технологий.

Литература:

1. Волков В.Э. Публично-правовое регулирование цифровых технологий: блокчейн, искусственный интеллект, виртуальная реальность: учеб. пособие. – Самара: Изд-во Самарского ун-та, 2023. – 118 с.
2. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» // СЗ РФ. – 2006. – № 31. – Ст. 3452.
3. Дремлюга Р.И. Виртуальная реальность: общие проблемы правового регулирования // Актуальные проблемы российского права. – 2020. – № 9. – С. 39–49.
4. В Совете Федерации обсудили правовые аспекты регулирования метавселенных. – URL: http://council.gov.ru/events/main_themes/138419/ (дата обращения: 09.03. 2024).
5. Афанасьева Е. А. Правовое регулирование виртуальной и дополненной реальности (обзор) // Право будущего: Интеллектуальная собственность, инновации: Ежегодник. Сер. «Правоведение». Вып. 1. / Ответ. ред. Е.Г. Афанасьева. – М.: Институт научной информации по общественным наукам РАН, 2018. – С. 166–172.
6. Иллюзия конфиденциальности в дополненной и виртуальной реальности. – URL: https://rdc.grfc.ru/2021/09/illuzia_konfidenzialnosti_v_dopolnennoy_i_virtualnoy_realnosti/?ysclid=llsogiw54v93131147 (дата обращения: 14.03.2024).
7. Смолин А.А., Жданов Д.Д., Потемин И.С., Меженин А.В., Богатырев В.А. Системы виртуальной, дополненной и смешанной реальности: учеб. пособие. – СПб.: Ун-тет ИТМО, 2018. – 59 с.
8. Риски безопасности и конфиденциальности в виртуальной и дополненной реальности. – URL: https://www.kaspersky.ru/resource-center/threats/security-and-privacy-risks-of-ar-and-vr?ysclid=lj8z4dbivp784970524 (дата обращения: 10.03.2024).

Legal Regulation of Personal Data Protection in Virtual and Augmented Realities

Aleksandrova A.S.
Samara National Research University named after academician S.P. Korolev

The purpose of the article is to form approaches to the legal regulation of personal data processing issues in the context of the spread of virtual and augmented reality (VR/AR) technologies. The author points to the increased interest and rapidly growing popularity of virtual and augmented reality (VR/AR) technologies in society, which allow you to get realistic impressions that blur the lines between the physical and digital worlds. Due to the rapid integration of these technologies into everyday life, very difficult issues arise related to the protection of users' personal data. The need to increase the level of personal data protection in the context of the proliferation of virtual/augmented reality technologies in the near future will pose new challenges in the areas of law-making and law enforcement.

The relevance of the study lies in the fact that when using VR/AR technologies, the security of users' personal data may be exposed to serious risks. The author justified the need to expand the capabilities of users to manage personal data when using VR/AR devices, as well as the adoption by the state of proactive measures to protect the personal data of its citizens. The author analyzes and compares the types of personal data of persons using VR/AR technologies, as well as the degree of growth of privacy threats in the event of a possible information leak. The existing regulatory framework for ensuring the protection of personal data in the Russian Federation was also analyzed and the need for further legal initiatives in this area was identified.

The author proposed a set of measures aimed at ensuring the privacy of users of virtual and augmented reality technologies.

Key words: legal regulation, information technology, personal data, confidentiality, virtual reality, augmented reality, privacy