

ПРИВАТНОСТЬ И ЗАЩИТА ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ В ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

В. С. Долунц

Московский государственный юридический университет имени О. Е. Кутафина

PRIVACY AND PROTECTION OF USER DATA IN VIRTUAL REALITY

V. S. Dolunts

Moscow State Law University named after O. E. Kutafin

Аннотация: рассматривается проблема защиты конфиденциальности персональных данных в виртуальной реальности в свете действующего российского законодательства. Анализируется российский и зарубежный правовой опыт. Делается вывод о необходимости усовершенствования их адаптации к сложным технологическим реалиям. Целью исследования является предложение возможных методов для решения данных вопросов. Посредством применения диалектического, социологического, системного, сравнительно-правового и иных методов автор приходит к заключению, что в качестве одного из механизмов разработки будущего законодательства возможен метод сорегулирования, который может способствовать безопасности и сохранению конфиденциальности данных в сфере VR. Такой подход может обеспечить лучшую правовую защиту и помочь решить текущие проблемы в этой области.

Ключевые слова: виртуальная реальность, дополненная реальность, Большие данные, Искусственный интеллект, Интернет вещей, персональные данные, конфиденциальность, защита данных.

Abstract: this article examines the issue of protecting the confidentiality of personal data in virtual reality within the framework of current Russian legislation. The author analyzes Russian and foreign legal experiences and concludes that there is a need to improve their adaptation to complex technological realities. The aim of the research is to propose possible methods to address these issues. Through the use of dialectical, sociological, systemic, comparative legal and other methods, the author comes to the conclusion that as one of the mechanisms for developing future legislation, a co-regulation method is possible, which can contribute to the security and preservation of data confidentiality in the field of VR. According to the author, such an approach could provide better legal protection and help address current challenges in this area.

Key words: virtual reality, augmented reality, Big Data, Artificial Intelligence, Internet of Things, personal data, confidentiality, data protection.

Развитие информационных технологий без сомнений можно считать главным достижением человечества XX–XXI вв. Их применение способствует существенному снижению трудозатрат, повышению безопасности и осведомленности человека и общества. Крупнейшие компании всего мира уже сегодня активно применяют новые технологии в своей деятельности. Это в равной степени справедливо относится и

к технологиям виртуальной и дополненной реальности (AR и VR).

Эти весьма схожие технологии уже сегодня нашли свое применение в самых различных отраслях, начиная с компьютерных игр и заканчивая промышленностью. По мнению эксперта журнала «Forbes» Джеймса Каплана, виртуальная реальность может быть использована многими компаниями для демонстрации своих новых продуктов, предоставляя тем самым возможность их клиентам со всего мира заранее озна-

комиться с такими продуктами. Это, как заявляет эксперт, существенно укрепляет связи между компаниями и их клиентами¹.

Использование технологий виртуальной реальности способно оказать позитивное воздействие и на правовую среду. В частности, по мнению Д. А. Степаненко и А. А. Митрофанова, виртуальная среда может быть использована в целях компьютерного моделирования, позволяющего визуализировать реконструкцию криминального события, при проведении таких процессуальных действий, как проверка показаний на месте, следственный эксперимент, ситуационные судебные экспертизы. По мнению ученых-криминалистов, компьютерно-опосредованная реальность может быть полезна и при проведении осмотров мест происшествий, предъявлений для опознания, допросов и очных ставок².

Вместе с тем использование технологий виртуальной реальности порождает и ряд правовых дискуссий. На сегодняшний день все еще остаются нерешенными вопросы защиты авторских прав на результаты интеллектуальной деятельности в виртуальной реальности, ответственности за действия в виртуальной реальности, рекламы, вопросы международного характера и многие другие вопросы.

Кроме того, применение технологий виртуальной реальности, как правило, сопровождается применением других передовых технологий, таких как Большие данные (BigData), Искусственный интеллект (ИИ) и Интернет вещей (IoT).

Большие данные – это сложные и большие наборы данных (часто из технологических устройств, таких как телефоны, медицинские устройства, устройства VR, собирающие и передающие данные), которые предприятия и организации анализируют для выявления закономерности в поведении потребителей и формирования бизнес-стратегий³. Примерами данных,

собираемых с помощью устройств VR, являются: походка, движение глаз, поведенческие данные о том, как пользователь реагирует на различные виртуальные ситуации⁴.

Искусственный интеллект – еще одна передовая технология, основной задачей которой является имитация когнитивных функций человека. Использование ИИ в виртуальной среде возможно, в частности, для генерации виртуальной среды, взаимодействия с участниками виртуальной реальности, управления элементами в данной среде и пр.

Интернет вещей – это система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека.

Речь идет не только о ноутбуках и смартфонах. Почти все устройства с кнопкой включения/выключения потенциально могут подключиться к интернету и стать частью Интернета вещей. Например, частью Интернета вещей могут стать человек с имплантом для мониторинга сердца, камера, ведущая наблюдение за жизнью диких животных в прибрежных водах, или автомобиль со встроенными датчиками, предупреждающими водителя о потенциальных рисках. По сути, это может быть любой объект, которому можно назначить сетевой адрес (IP-адрес) и который может передавать данные по сети⁵.

Таким образом, все три описанные технологии имеют дело с данными. Эти данные передаются от одного оператора к другому, анализируются, подвергаются тем или иным манипуляциям, что приходится по духу далеко не всем пользователям. Указанные технологии, к сожалению, пока не имеют универсального регулирования, способного обеспечить интересы и пользователей, и разработчиков, поставщиков товаров и услуг. По состоянию на февраль 2024 г. не только российское, но и зарубежное законодательство пока не пришло к консенсусу по вопросу совместимости современных технологий с имеющимися нормативными нормами.

⁴ См.: O'Brolcháin F., Jacquemard T., Monaghan D., O'Connor N., Novitzky P., Gordijn B. The Convergence of Virtual Reality and Social Networks : Threat to Privacy and Autonomy // *Sci Eng'g Ethics*. 2016. Vol. 22, №. 1. P. 3–4 ; Ciproso P, Giglioli IAC, Raya MA, Riva G. The Past, Present, and Future of Virtual and Augmented Reality Research : A Network and Cluster Analysis of the Literature // *Frontiers Psychol*. 2018. Vol. 9. №. 1. P. 3.

⁵ См.: URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-iot> (дата обращения: 24.01.2024).

¹ См.: URL: <https://www.forbes.com/sites/forbestechcouncil/2022/12/05/13-productive-and-creative-uses-for-vr-that-impress-tech-experts/?sh=1a64255e32f9> (дата обращения: 24.01.2024).

² См.: Степаненко Д. А., Митрофанова А. А. Цифровизация как фактор и условие развития современной криминалистики // *Рос. следователь*. 2023. № 4. С. 16–22.

³ См.: Nimrod K. Big Data, Consumer Behavior and the Consumer Packaged Goods Blindspot // *Forbes*. 2019. URL: <https://www.forbes.com/sites/forbestechcouncil/2019/09/05/big-data-consumer-behavior-and-the-consumer-packaged-goods-blindspot/> (дата обращения: 24.01.2024).

Особую важность, как было отмечено, имеет вопрос конфиденциальности пользователей, защиты их данных от неправомерного и избыточного сбора и обработки. Сегодня, когда крупные ИТ-компании имеют практически безграничный доступ к данным о пользователях, вопрос защиты их данных становится всё более остро.

Персональные данные и информационная среда

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)⁶. Именно так определяет понятие персональных данных основной закон Российской Федерации в области персональных данных.

Предлагаемое российским законодателем определение является достаточно широким для того, чтобы отнести к персональным данным в том числе сведения об электронной почте, номере телефона, страницы в социальных сетях и другие сведения, которые могут создать ассоциацию с определенным физическим лицом.

В контексте информационной среды, и виртуальной реальности в частности, возникает достаточно объективный вопрос: являются ли данные о передвижениях, местоположении, предпочтениях, манерах походки, передвижения глаз данными персональными? Виртуальная реальность позволяет пользователям погружаться в цифровые миры, в то же время она собирает разнообразные данные о поведении и взаимодействии пользователей. Эти данные могут включать в себя информацию о движениях, голосе, реакциях, предпочтениях, даже физиологических показателях. Даже без применения технологий виртуальной реальности крупные ИТ-компании, среди которых Apple, Microsoft, Google, завалены коллективными исками пользователей за незаконный сбор данных о них.

Обращаясь к российскому правовому полю, стоит привести в пример дело против «LinkedIn Corporation». Решением Таганского районного суда г. Москвы был ограничен доступ к интернет-ресурсу <http://www.linkedin.com>. В дальнейшем Судебной коллегией по гражданским делам Московского городского суда данное решение было оставлено в силе. Изначально с иском в

суд первой инстанции обратилась Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Нарушения, по мнению истца, выразились в сборе персональной информации о пользователях указанного ресурса и гражданах, не являющихся пользователями, в ее использовании и передаче без соответствующего согласия и с нарушениями положений Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», касающиеся принципов и условий обработки персональных данных в России⁷. В частности, «LinkedIn Corporation» использовались cookie файлы (небольшие фрагменты текста, передаваемые в браузер с сайта, который пользователь открывает⁸), сведений о поведении пользователя на странице и сведений о местонахождении.

К аналогичному заключению пришел и арбитражный суд г. Москвы в своем решении против ПАО «МГТС». В соответствии с материалами дела ООО «ОБМР» получало от ПАО «МГТС» следующие сведения об абонентах: случайный идентификатор (Cookie «UID») в HTTP-запросе (протокол прикладного уровня передачи данных) пользователя, позволяющий отличить трафик пользователя от трафика других пользователей для получения списка его предпочтений; IP-адрес из IP-пакета HTTP-запроса пользователя, позволяющий получить географическое положение пользователя с точностью определения до названия населенного пункта и др. Из представленной оператором связи информации, относящейся к абонентам, ООО «ОБМР» формирует предпочтения конкретного абонента и передает данную информацию потенциальным рекламодателям для того, чтобы они показывали рекламу именно определенному абоненту, сведения о котором ранее были предоставлены оператором связи ПАО «МГТС». В своем решении суд указывает, что такая обработка данных позволяет косвенно определить субъекта персональных данных, которому впоследствии рекламодатель персонифицированно, т.е. определенному лицу, направляет определенную рекламу в зависимости от предпочтений субъекта, а именно – ранее просмотренных субъектом ин-

⁶ О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ. Доступ из справ.-правовой система «КонсультантПлюс».

⁷ См.: URL: <https://m.mos-gorsud.ru/mgs/news/e5825bb6-d15d-4512-a158-bdfdb910e82c> (дата обращения: 24.01.2024).

⁸ См.: URL: <https://policies.google.com/technologies/cookies?hl=ru> (дата обращения: 24.01.2024).

тернет-страниц, товаров, работ, услуг, рекламируемых в сети Интернет и т. п.⁹

Подобная судебная практика имеет место не только в России. К аналогичным заключениям пришли и зарубежные суды.

Так, в январе 2022 г. четырьмя генпрокурорами США был подан иск на компанию Google за отслеживание компанией местоположения пользователей без их согласия. По мнению истцов, суд должен оштрафовать Google и заставить компанию удалить полученные данные. Об этом сообщил телеканал CNBC. В Google все обвинения отвергают – там заявили, что они лишь обеспечивали надежный контроль данных о местоположении. Как сказано в иске, гаджеты Google не предоставляли пользователям информацию о сборе данных об их местоположении. Более того, гаджеты продолжали отслеживать местоположение пользователей даже после прямого запрета это делать¹⁰.

Еще одним примером является судебное дело «Google и сбор данных с Wi-Fi сетей». В 2010 г. Google была обвинена в сборе данных с Wi-Fi сетей без согласия пользователей во время съемки для службы Street View. Это привело к расследованиям и судебным спорам в различных странах. Итогом разбирательства стал вынесенный компании Google штраф в размере 7 млн долларов США¹¹.

Не менее громким стало судебное дело «Vizio и сбор данных с телевизоров». В 2017 г. компания Vizio была обвинена в сборе данных о просмотренных пользователями программах и передачах через свои телевизоры без согласия пользователей. В результате компания согласилась заплатить штраф и изменить практики¹².

Это лишь несколько примеров судебных дел и инцидентов, связанных с отслеживанием активности пользователей различных сервисов. Указанное явно свидетельствует о существую-

щей проблеме, появление которой обязано развитию информационных технологий, в числе которых и технологии виртуальной реальности.

На сегодняшний день иски, связанные с нарушением конфиденциальности пользователей VR, не являются столь популярными, однако это не означает отсутствия необходимости превентивного регулирования данной сфере, которое в достаточной степени будет учитывать как права и интересы компаний-разработчиков, так и их пользователей.

Персональные данные и виртуальная реальность

Как отмечалось ранее, для формирования виртуальных элементов или виртуальных миров в трехмерном пространстве в целом, технология VR требуются определенные данные, представляемые со стороны пользователя. Такие данные представляют из себя не единичный, а постоянный поток данных, генерируемый пользователем во время взаимодействия с виртуальной средой. Эти данные могут включать в себя информацию о местоположении, его изменении, личные данные пользователя и даже информацию, получаемую с помощью технологии отслеживания взгляда, технологии «Интерфейс мозг-компьютер», представляющую из себя инвазивные или неинвазивные технологии, позволяющие преобразовывать некоторые нейрофизиологические сигналы в команды, адресованные внешнему техническому устройству или компьютеру¹³. В совокупности объем и масштаб сбора пользовательских данных, необходимых для основных функций VR, отличают эти технологии от других потребительских устройств и приложений.

Вместе с тем важно отметить, что по состоянию на сентябрь 2023 г. в Российской Федерации отсутствует полноценное и подробное законодательство, специфически регулирующее виртуальную реальность. В ноябре 2022 г. Министерство внутренних дел России предложило принять закон, регулирующий использование систем виртуальной реальности. Принятие закона, по мнению Министерства внутренних дел России, необходимо ввиду возможных рисков деструктивного воздействия вирту-

⁹ URL: https://kad.arbitr.ru/Document/Pdf/898157da-8f67-4c18-8a6b-d74d68162eac/A40-14902-2016_20160311_Reshenija%20i%20postanovlenija.pdf?isAddStamp=True (дата обращения: 24.01.2024).

¹⁰ См.: URL: <https://secretmag.ru/news/na-google-podali-v-sud-iz-za-slezhki-za-polzovatelyami-pogeolokacii-25-01-2022.htm> (дата обращения: 24.01.2024).

¹¹ См.: URL: https://www.vedomosti.ru/technology/articles/2013/03/13/google_zaplatit_v_ssha_shtraf_v_7 mln_za_sbor_dannyh_iz (дата обращения: 24.01.2024).

¹² См.: URL: <https://www.cableman.ru/content/vizio-oshtrafovali-za-sbor-dannykh-polzovatelei-internet-podklyuchennykh-tv> (дата обращения: 24.01.2024).

¹³ См.: Мокшенко О. А., Черникова Л. А., Фролов А. А. Интерфейс мозг-компьютер как новая технология нейрореабилитации // *Анналы клинической и экспериментальной неврологии*. 2011. № 3. С. 46–52.

альной реальности на человека¹⁴. В частности, Министерством внутренних дел России предлагается ввести маркировку компьютерного и другого развлекательного контента в дополнение к возрастным ограничениям, а также наделить юридическим статусом кибердружины, т. е. добровольцев, выявляющих в интернете деструктивный, по их мнению, контент¹⁵.

Подобная инициатива в то же время требует детального осмысления. В первую очередь предложенная инициатива является достаточно узконаправленной и сложно реализуемой. Реализация системы маркировки требует финансовых и технических ресурсов. Создание и поддержание эффективной системы может быть сложной задачей для провайдеров интернет-услуг и других организаций. Не менее важными проблемами остаются прозрачность и объективность маркировки. Процесс маркировки контента должен быть прозрачным и объективным. Однако в реальности могут возникать ситуации, когда маркировка происходит субъективно или даже произвольно, что может приводить к несправедливым ограничениям для некоторых пользователей или сообществ. Кроме того, всё еще остаются нерешенными вопросы защиты персональных данных участников среды виртуальной реальности. Маркировка и обработка персональных данных пользователей – это процессы, связанные с сбором, хранением, анализом и использованием личной информации о пользователях в сети интернет. В свете обеспечения конфиденциальности и соблюдения законов о защите данных эти процессы становятся сложным вопросом. Важно соблюдать определенные принципы и стандарты для обработки персональных данных.

Юридическая доктрина, к сожалению, пока также не пришла к единому умозаключению по модели правового регулирования отношений с использованием технологий VR. Проблема разработки такой модели в первую очередь обусловлена сложностью используемых технологий, их специфичностью. Одним из примеров такой ситуации является технология BigData. Дело в том, что действующее законодательство Российской

Федерации не приспособлено к данной технологии. По верному замечанию А. В. Минбалева и В. А. Филоненковой, персональные данные нередко обрабатываются с помощью технологии BigData. В качестве решения данной проблемы ученые видят необходимость уведомления Роскомнадзора со стороны компаний, планирующих такое использование персональных данных, а также выделение данной цели в процессе обработки персональных данных и получения специального согласия субъекта персональных данных¹⁶.

А. И. Савельев полагает, что в силу своего большого объема и быстроты формирования и обработки большие данные несовместимы как с принципом ограничения обработки персональных данных заранее определенными целями, так и с концепцией информированного, конкретного и сознательного согласия на легитимную обработку персональных данных. Вследствие этого автор делает вывод о неадекватности современного регулирования отношений по использованию больших данных¹⁷.

Аналогичную ситуацию можно наблюдать и с иными технологиями, используемыми в виртуальной реальности, в том числе и искусственным интеллектом, который обрабатывает миллиарды терабайты информации.

Стоит отметить, что подобная ситуация наблюдается не только в России, но и за рубежом. Политический аналитик в области технологий и киберполитики «ITIF» Элисс Дик, рассматривая федеральное законодательство США, приходит к выводу о необходимости принятия рекомендаций и разъяснений со стороны федеральных регулирующих органов о применимости действующего законодательства США к технологиям AR и VR¹⁸. Кроме того, по мнению аналитика необходимо также принятие технических мер со стороны поставщиков, направленных на защи-

¹⁶ См.: Минбалева А. В., Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети интернет в условиях пандемии // Вестник Южно-Урал. гос. ун-та. Серия: Право. 2020. № 3. С. 89–94.

¹⁷ См.: Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право : журнал Высшей школы экономики. 2015. № 1. С. 43–66.

¹⁸ См.: Dick E. Balancing User Privacy and Innovation in Augmented and Virtual Reality // Information technology & innovation foundation. 2021. URL: <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/> (дата обращения: 25.01.2024).

¹⁴ См.: URL: <https://www.pnp.ru/social/v-rossii-predlozhili-vvesti-regulirovanie-virtualnoy-realnosti.html> (дата обращения: 24.01.2024).

¹⁵ См.: URL: <https://www.pnp.ru/social/v-rossii-predlozhili-vvesti-regulirovanie-virtualnoy-realnosti.html> (дата обращения: 24.01.2024).

ту конфиденциальности потребителей. Вместе с тем Элисс Дик считает также необходимым реформировать и гармонизировать действующее законодательство в области конфиденциальности, не препятствуя при этом развитию технологий AR и VR¹⁹.

Рассматривая Общий регламент по защите данных Европейского Союза (GDPR), Йеджи Ким полагает, что данные в виртуальной реальности, скорее всего, считаются биометрическими данными²⁰. Ссылаясь на GDPR, автор указывает на статью 9(1), которая запрещает сбор биометрических данных, и на исключения, перечисленные в статье 9(2), одним из которых является «явное согласие»²¹. «Явное согласие» – это термин, предусмотренный GDPR, который устанавливает более высокий стандарт согласия, чем обычное согласие. «Явное согласие» требует «заявления или ... ясные позитивные действия». Согласно Руководству «EDPB», точный стандарт «явного согласия» еще не установлен. Тем не менее в Руководстве содержатся полезные примеры, которые можно квалифицировать как явное согласие. Слово «явное» относится к тому, как субъект данных выражает согласие: письменное заявление, телефонный разговор и электронная подпись квалифицируются как «явное согласие». Даже установка флажка «да» на веб-сайте, например, «настоящим я даю согласие на обработку моих данных», соответствует стандарту явного согласия²². Несмотря на то что стандарт явного согласия, безусловно, более строгий, чем стандарт обычного согласия, он, похоже, не создает особых сложностей для компаний, предлагающих услуги с использованием технологий виртуальной реальности, которым нужно будет всего лишь создать простое всплывающее окно с четким заявлением о согласии²³.

Более того, как отмечает Йеджи Ким, цель политики GDPR направлена на обеспече-

ние гибкости правил для новых технологий. Европейский орган по надзору за защитой данных (EDPS) недавно опубликовал официальный документ по ИИ, в котором говорится, что GDPR «технологически нейтрален» и «не является препятствием для успешного внедрения новых технологий, в частности ИИ»²⁴. Автор также обращает внимание, что, хотя в официальном документе виртуальная реальность напрямую не обсуждается, виртуальная реальность и ИИ очень тесно связаны. Для обработки данных виртуальной реальности требуется анализ ИИ. Более того, в официальном документе демонстрируется стремление к гибкости новых технологий в целом²⁵.

Решением указанной проблемы Йеджи Ким видит в предоставлении пользователю возможности устанавливать свои параметры конфиденциальности, а также в установлении интерактивных упражнений, проверяющих понимание пользователями представленного видео, которые не позволят пользователям прокручивать страницу вниз, не ознакомившись с политикой конфиденциальности²⁶.

Технологии виртуальной реальности (VR) представляют собой важное направление в развитии информационных технологий. На данный момент основной областью применения VR являются компьютерные игры. Тем не менее, как указывалось ранее, VR-технологии обладают потенциалом для общественно-полезных целей.

Объективное исследование действующего законодательства в России и других странах свидетельствует о том, что нормы, регулирующие технологии VR, находятся в стадии развития и ограничены. Это создает необходимость в более глубоком анализе со стороны законодательных органов. Однако разработка будущей модели регулирования не может осуществляться в изоляции от рынка VR. Компании-разработчики и предоставляющие услуги в этой сфере должны активно участвовать в формировании будущего законодательства.

¹⁹ См.: *Dick E.* Op. cit.

²⁰ См.: *Yeji K.* Virtual Reality Data and Its Privacy Regulatory Challenges : a Call to Move Beyond Text-Based Informed Consent // University of California, Berkeley, School of Law. 2022. Vol. 110. P. 225–256.

²¹ См.: General Data Protection Regulation (GDPR). URL: <https://gdpr-info.eu/> (дата обращения: 25.01.2024).

²² См.: European Data Prot. Bd. Guidelines 05/2020 on Consent under Regulation 2016/679 // ¶ 92 (May 4, 2020). URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (дата обращения: 25.01.2024).

²³ См.: *Yeji K.* Op. cit.

²⁴ См.: European Data Prot. Supervisor. EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European Approach to Excellence and Trust: сокращение имени организации // ¶ 16 (June 29, 2020). URL: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf (дата обращения: 25.01.2024).

²⁵ См.: *Ibid.*

²⁶ См.: *Yeji K.* Op. cit.

В то же время наиболее целесообразным методом создания будущей правовой базы является метод сорегулирования, который включает в себя участие как государства, так и рынка технологий виртуальной реальности. Этот метод позволит достичь консенсуса, учитывая интересы как компаний, так и пользователей, где государство будет выступать защитником интересов общества.

Явным фактом является, что компании, стремясь к прибыли, могут применять простые и иногда неправомерные методы. В этом контексте использование метода саморегулирования, где компании-разработчики формируют правила использования цифровой среды, в данном случае VR, исключительно с их стороны, является рискованным, так как это может создать неблагоприятное положение для пользователей.

С другой стороны, исключительное государственное регулирование виртуальной среды может ограничить развитие технологий VR и стать невыгодным как для компаний-разработчиков, так и для конечных потребителей. Это может привести к замедлению прогресса в области информационных технологий, что не является выгодным ни для государства, ни для разработчиков, ни для пользователей.

Библиографический список

General Data Protection Regulation (GDPR). URL: <https://gdpr-info.eu/>

European Data Protection Supervisor. «EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European Approach to Excellence and Trust» ¶ 16 (June 29, 2020). URL: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

European Data Prot. Bd. Guidelines 05/2020 on Consent under Regulation 2016/679 // 92 (May 4, 2020). URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Минбалева А. В., Филоненкова В. А. Проблемы защиты персональных данных и цифрового профиля человека в сети интернет в условиях пандемии // Вестник Южно-Урал. гос. ун-та. Серия: Право. 2020. № 3. С. 89–94.

Мокиенко О. А., Черникова Л. А., Фролов А. А. Интерфейс мозг-компьютер как новая технология нейрореабилитации // Анналы клинической и экспериментальной неврологии. 2011. № 3. С. 46–52.

Савельев А. И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право: журнал Высшей школы экономики. 2015. № 1. С. 43–66.

Степаненко Д. А., Митрофанова А. А. Цифровизация как фактор и условие развития современной криминалистики // Рос. следователь. 2023. № 4. С. 16–22.

Cipresso P, Giglioli IAC, Raya MA, Riva G. The Past, Present, and Future of Virtual and Augmented Reality Research : a Network and Cluster Analysis of the Literature // Frontiers Psychol. 2018. Vol. 9, №. 1.

Dick E. Balancing User Privacy and Innovation in Augmented and Virtual Reality // Information technology & innovation foundation. 2021. URL: <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/>

O'Brolcháin F., Jacquemard T., Monaghan D., O'Connor N., Novitzky P., Gordijn B. The Convergence of Virtual Reality and Social Networks : Threat to Privacy and Autonomy // Sci Eng'g Ethics. 2016. Vol. 22, № 1. P. 3–4.

Nimrod K. Big Data, Consumer Behavior and the Consumer Packaged Goods Blindspot // Forbes. 2019. URL: <https://www.forbes.com/sites/forbestechcouncil/2019/09/05/big-data-consumer-behavior-and-the-consumer-packaged-goods-blindspot/>

Yeji K. Virtual Reality Data and Its Privacy Regulatory Challenges : a Call to Move Beyond Text-Based Informed Consent // University of California, Berkeley, School of Law. 2022. Vol. 110. P. 225–256.

URL: <https://www.pnp.ru/social/v-rossii-predlozhili-vvesti-regulirovanie-virtualnoy-realnosti.html>

URL: <https://www.forbes.com/sites/forbestechcouncil/2022/12/05/13-productive-and-creative-uses-for-vr-that-impress-tech-experts/?sh=1a64255e32f9>

URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-iot>

URL: <https://m.mos-gorsud.ru/mgs/news/e5825bb6-d15d-4512-a158-bdfdb910e82c>

URL: <https://policies.google.com/technologies/cookies?hl=ru>

URL: https://kad.arbitr.ru/Document/Pdf/898157da-8f67-4c18-8a6b-d74d68162eac/A40-14902-2016_20160311_Reshenija%20i%20postanovlenija.pdf?isAddStamp=True

RL: <https://secretmag.ru/news/na-google-podali-v-sud-iz-za-slezhki-za-polzovatelyami-po-geolokacii-25-01-2022.htm>

URL: https://www.vedomosti.ru/technology/articles/2013/03/13/google_zaplatit_v_ssha_shtraf_v_7 mln_zh_sbor_dannyh_iz

URL: <https://www.cableman.ru/content/vizio-oshtrafovali-za-sbor-dannykh-polzovatelei-internet-podklyuchennykh-tv>

References

General Data Protection Regulation (GDPR) URL: <https://gdpr-info.eu/>

European Data Protection Supervisor. «EDPS Opinion on the European Commission’s White Paper on Artificial Intelligence – A European Approach to Excellence and Trust» ¶ 16 (June 29, 2020). URL: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf

European Data Prot. Bd. Guidelines 05/2020 on Consent under Regulation 2016/679 // 92 (May 4, 2020). URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Minbaleev A. V., Filonenkova V. A. Problems of protecting personal data and a person’s digital profile on the Internet during a pandemic // Bulletin of SUSU. Series: Law. 2020. № 3. P. 89–94.

Mokienko O. A., Chernikova L. A., Frolov A. A. Brain-computer interface as a novel tool of neurorehabilitation // Annals of Clinical and Experimental Neurology. 2011. № 3. P. 46–52.

Savel'yev A. I. Problems of applying legislation on personal data in the era of «Big Data» // Law. Journal of the Higher School of Economics. 2015. № 1. P. 43–66.

Stepanenko D. A., Mitrofanova A. A. Digitalization as a factor and condition for the development of modern criminology // Russian investigator. 2023. № 4. P. 16–22.

Cipresso P, Giglioli IAC, Raya MA, Riva G. The Past, Present, and Future of Virtual and Augmented Reality Research : a Network and Cluster Analysis of the Literature // Frontiers Psychol. 2018. Vol. 9, № 1.

Dick E. Balancing User Privacy and Innovation in Augmented and Virtual Reality // Information technology & innovation foundation. 2021. URL: <https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/>

O’Brolcháin F., Jacquemard T., Monaghan D., O’Connor N., Novitzky P., Gordijn B. The Convergence of Virtual Reality and Social Networks : Threat to

Privacy and Autonomy // Sci Eng’g Ethics. 2016. Vol. 22, № 1. P. 3–4.

Nimrod K. Big Data, Consumer Behavior and the Consumer Packaged Goods Blindspot // Forbes. 2019. URL: <https://www.forbes.com/sites/forbestechcouncil/2019/09/05/big-data-consumer-behavior-and-the-consumer-packaged-goods-blindspot/>

Yeji K. Virtual Reality Data and Its Privacy Regulatory Challenges : a Call to Move Beyond Text-Based Informed Consent. // University of California, Berkeley, School of Law. 2022. Vol. 110. P. 225–256.

URL: <https://www.pnp.ru/social/v-rossii-predlozhili-vvesti-regulirovanie-virtualnoy-realnosti.html>

URL: <https://www.forbes.com/sites/forbestechcouncil/2022/12/05/13-productive-and-creative-uses-for-vr-that-impress-tech-experts/?sh=1a64255e32f9>

URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-iot>

URL: <https://m.mos-gorsud.ru/mgs/news/e5825bb6-d15d-4512-a158-bdfdb910e82c>

URL: <https://policies.google.com/technologies/cookies?hl=ru>

URL: https://kad.arbitr.ru/Document/Pdf/898157da-8f67-4c18-8a6b-d74d68162eac/A40-14902-2016_20160311_Reshenija%20i%20postanovlenija.pdf?isAddStamp=True

URL: <https://secretmag.ru/news/na-google-podali-v-sud-iz-za-slezhki-za-polzovatelyami-po-geolokacii-25-01-2022.htm>

URL: https://www.vedomosti.ru/technology/articles/2013/03/13/google_zaplatit_v_ssha_shtraf_v_7 mln_za_sbor_dannyh_iz

URL: <https://www.cableman.ru/content/vizio-oshtrafovali-za-sbor-dannykh-polzovatelei-internet-podklyuchennykh-tv>

Московский государственный юридический университет имени О. Е. Кутафина

Долунц В. С., аспирант кафедры информационного права и цифровых технологий

E-mail: vartan.dolunts@gmail.com

Поступила в редакцию: 07.02.2024

Для цитирования:

Долунц В. С. Приватность и защита данных пользователей в виртуальной реальности // Вестник Воронежского государственного университета. Серия: Право. 2024. № 2 (57). С. 131–138. DOI: <https://doi.org/10.17308/law/1995-5502/2024/2/131-138>.

Moscow State Law University named after O. E. Kutafin

Dolunts V. S., Post-graduate Student of the Department of Information Law and Digital Technologies

E-mail: vartan.dolunts@gmail.com

Reserved: 07.02.2024

For citation:

Dolunts V. S. Privacy and protection of user data in virtual reality // Proceedings of Voronezh State University. Series: Law. 2024. № 2 (57). P. 131–138. DOI: <https://doi.org/10.17308/law/1995-5502/2024/2/131-138>.