- ТЕОРИЯ УПРАВЛЕНИЯ -

Дата поступления рукописи в редакцию: 28.09.2025 г.
Дата принятия рукописи в печать: 15.10.2025 г.
DOI: 10.24412/2782-3830-2025-9-134-137

ОВАКАНЯН Лиана Кимиковна,
Московский государственный университет имени М.В. Ломоносова,
Высшая школа государственного аудита (факультет),
аспирант кафедры компьютерного права и
информационной безопасности,
e-mail: mail@law-books.ru

МЕТАВСЕЛЕННАЯ КАК ОБЪЕКТ ПРАВОВОГО РЕГУЛИРОВАНИЯ: СПЕЦИФИКА ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Аннотация. *Статья развивает правозащитный и институциональный подход к регулированию обработки персональных данных в метавселенных, рассматривая их как персистентные и по умолчанию трансграничные цифровые среды с иммерсивными интерфейсами и алгоритмическим управлением. Аргументируется необходимость увязать конституционные гарантии частной жизни с технологически нейтральными инструментами российского права, усилив режим обработки биометрических и сенсорно-поведенческих «иммерсивных данных», внедрив механизм иммерсивного согласия, оценку воздействия на защиту данных и алгоритмического риска. Предлагается развернуть экстерриториальные привязки защиты прав резидентов РФ, развить распределённую ответственность участников экосистемы и закрепить стандарты интероперабельности и переносимости активов между платформами.*

Ключевые слова: *метавселенная, иммерсивные данные, виртуальные миры, виртуальная реальность, дополненная реальность, биометрические персональные данные, экстерриториальность, трансграничная передача персональных данных.*

OVAKANYAN Liana Kimikovna,
Lomonosov Moscow State University,
Higher School of Public Audit (Faculty),
PhD Candidate, Department of Computer
Law and Information Security

THE METAVERSE AS A MATTER OF LEGAL REGULATION: SPECIFICS OF PERSONAL DATA PROCESSING

Annotation. *The article adopts a rights-based, institutional perspective on regulating personal-data processing in metaverses understood as persistent, default cross-border environments with immersive interfaces and algorithmic governance. It argues for aligning constitutional privacy guarantees with Russia's technology-neutral legal tools by strengthening the regime for biometric and sensor-behavioral «immersive data», introducing an immersive consent mechanism, mandating Data Protection Impact Assessment and Algorithmic Impact Assessment, enabling a hybrid right to erasure for immutable ledgers. The paper proposes extending extraterritorial protections for Russian residents, developing distributed liability, and codifying interoperability and portability of identities/assets across platforms.*

Key words: *metaverse, immersive data, virtual worlds, virtual reality, augmented reality, biometrics, extraterritoriality, cross-border data transfer.*

Метавселенная как глобальное виртуальное пространство, объединяющее физическую и цифровую реальности, ставит перед правовой системой новые вызовы. Без чёткого понятийного аппарата невозможно выработать комплексную концепцию регулирования метавселенной, что ведёт к риску своего рода «цифрового луддизма» – торможения развития технологий из-за несовершенства законодательства.

Еще в 2013 году В. В. Архипов обозначил, что предметом виртуального права являются

правовые аспекты виртуальных миров – компьютерно моделируемых пространств, обеспечивающих возможность взаимодействия между пользователями [1]. Иными словами, правовая наука признала существование особой сферы отношений в виртуальной среде, требующей самостоятельного анализа. Развитие многопользовательских онлайн-миров и появление сложных цифровых экономик внутри них привело к тому, что виртуальные события могут иметь вполне реальные правовые последствия. Так, Ю. М. Батурин и С. В. Полубинская обращают внимание на многочисленные правонарушения в массовых многопользовательских виртуальных мирах и констатируют наличие серьёзных пробелов в их правовом регулировании [2]. Виртуальные преступления – кража цифровых объектов, мошенничество с виртуальными ценностями, причинение вреда чести и достоинству посредством аватаров и др. – становятся «реальными» в том смысле, что наносят ощутимый ущерб и требуют реагирования со стороны правопорядка. Это подчёркивает необходимость адаптации существующих правовых институтов к новой цифровой среде.

Метавселенная стала также качественно новым пространством обработки персональных данных: персистентные 3D-среды, непрерывное присутствие пользователей через аватары, сквозная идентичность и оборотоспособность цифровых объектов формируют «тотальную» телеметрию взаимодействия _ от координат движения, взгляда и мимики до биосигналов носимых устройств и контекстных аудио и видео-фрагментов, собираемых в режиме реального времени. Такая архитектура выводит на первый план не столько «новые» правовые категории, сколько необходимость последовательной реализации конституционных гарантий частной жизни в условиях иммерсивной сенсорики и алгоритмической модерации.

Российская доктрина последовательно исходит из технологической нейтральности регулирования: права и свободы личности первичны, а право должно уметь работать поверх сменяющихся технических поколений [6]. При этом действующее законодательство о персональных данных предоставляет базовые инструменты – принципы законности, соразмерности, ограничения целей и сроков хранения, безопасность и права субъекта (доступ, исправление, удаление, ограничение обработки) [5]. Задача правоприменителя и регулятора – «перевести» эти универсальные положения в требования к устройству сервисов дополненной или виртуальной реальности и процессам их эксплуатации, не изобретая избыточных исключений.

Фактическая специфика обработки персональных данных в метавселенной проявляется в трёх измерениях. Первое – чувствительность данных: сенсорно-поведенческие массивы способны устойчиво идентифицировать пользователя и реконструировать психофизиологический профиль, следовательно, значительная их часть тяготеет к биометрическим персональным данным и требует усиленных правовых оснований и мер их защиты. Второе – интенсивность и непрерывность обработки персональных данных: потоковость и контекстность телеметрии усиливают риски вторичного использования и переобучения алгоритмов вне совместимых целей, что требует строгой минимизации и сегментации хранилищ. Третье –трансграничность по умолчанию: распределённые дата-центры означают, что юридически значимые события регулярно выходят за пределы одной юрисдикции, а защита прав должна опираться на экстерриториальные привязки и коллизионные механизмы признания доказательств и исполнения решений [8].

В этих условиях представляется оправданным выделить на доктринальном и корпоративно-стандартном уровнях «иммерсивные данные» как подкатегорию персональных данных (без введения новой «особой категории» в законе), охватывающую телеметрию устройств дополненной реальности, биосигналы и производные эмоционально-поведенческие метрики, если они используются для принятия решений о пользователе. Для этой подкатегории устанавливаются усиленные гарантии: явное и контекстное согласие, обязательная оценка воздействия на защиту данных до начала высокорисковой обработки данных, запрет вторичного использования вне совместимых целей, псевдонимизация и шифрование по умолчанию, изоляция первичного и производного слоёв, короткие сроки хранения данных и прозрачная телеметрия доступа к данным [5].

Такой риск-ориентированный подход согласуется с отечественной линией на технологическую нейтральность и укладывается в действующие рамки Федерального закона № 152-ФЗ «О персональных данных» и подзаконных актов о защите персональных данных, не требуя изменить базовые конструкции [7].

Основанием для обработки персональных данных в метавселенной становится иммерсивное согласие: «клик-баннер» эпохи плоских интерфейсов не обеспечивает информированности и добровольности в метавселенной. Юридически значимое согласие должно возникать в момент события (активации сенсора/функции), быть модульным (по категориям и целям), обратимым («пауза» обработки без выхода из сцены), визуально понятным (например, индикаторы активных сенсоров) и сопровождаться журналом доступа, доступным самому пользователю [4].

Алгоритмическая модерация и рекомендательные системы формируют второй блок риска.

Когда автоматизированные решения затрагивают доступ к функциям, цены, санкции для аватара или видимость контента, требуется процедурная алгоритмическая подотчётность: описание моделей, метрики точности и недискриминации, запрет на принятие юридически значимых решений исключительно на основании технологий искусственного интеллекта. Эти механизмы целесообразно встраивать в системы управления конфиденциальностью на базе национально принятых стандартов, обеспечивая сквозной контроль за жизненным циклом данных – от сбора до удаления.

Трансграничная передача данных по умолчанию объективно усиливает значение локализации первичных баз, правомерных сценариев последующей передачи и коллизионных оговорок. Российское законодательство обязывает операторов обеспечивать сбор персональных данных граждан РФ на территории страны, а трансграничная передача допускается при соблюдении установленных условий; для метавселенных это практически означает сегментацию хранилищ (разделение идентификаторов и потоков), псевдонимизацию при маршрутизации и договорные гарантии получателя, дополненные техническими средствами контроля [1]. Системно важно закрепить экстерриториальные привязки применимости национальных требований к обработке данных резидентов Российской Федерации вне зависимости от юрисдикции оператора, а также типовые процессуальные оговорки признания цифровых доказательств и исполнение решений в трансграничной среде [8].

Правовая ответственность в многооператорной архитектуре метавселенных требует раздвоенного контура: в частноправовом – матрицы ролей, договорные обязательства по безопасности, реагирование на инцидент и уведомление субъектов, страховые механизмы покрытия вреда и техническая подотчётность; в публично-правовом – требования к высокорисковым видам обработки данных, координация с надзорными органами при трансграничных инцидентах и прозрачность модерации. Для децентрализованных автономных организаций доктринально оправдана конструкция «кооперативного оператора» – совокупности лиц, совместно определяющих цели и способы обработки через голосование и смарт-контракты, с распределением ответственности и страховыми фондами [6].

Субстантивная защита идентичности в метавселенной включает и гражданско-правовую охрану «репутационной оболочки» аватара: вмешательство в идентичность затрагивает нематериальные блага и имущественные интересы; применим инструментарий защиты чести, достоинства и деловой репутации с адаптацией средств пресечения (блокировка контрафактных 3D-моделей, восстановление доступа, возмещение убытков) и с учётом доказательной специфики цифровой сцены [3].

Наконец, модальность «интероперабельность и переносимость» —– правовое условие конкуренции и предотвращения платформенного «запирания». Право пользователя на перенос своих данных, идентичности и цифрового инвентаря между совместимыми платформами при наличии открытых форматов снижает риски злоупотребления доминированием и усиливает реальную управляемость данными самим субъектом – это логичное развитие принципов справедливости обработки и участия личности в контроле над информацией о себе [4]. В сумме вырисовывается практика-ориентированная «карта» регулирования: технологически нейтральная основа, усиленный режим защиты иммерсивных данных, иммерсивное согласие как обязательный стандарт обработки данных в метавселенной, оценка рисков для высокорисковых функций, экстерриториальные привязки и признание цифровых доказательств, распределённая ответственность и поощрение интероперабельности. Такой подход не подменяет фундамент права «новыми категориями», а обеспечивает реальную исполнимость классических гарантий личности в условиях иммерсивной архитектуры, согласуя конституционную оптику с техническими и организационными мерами защиты.

Список литературы:

[1] Архипов В. В. Виртуальное право: основные проблемы нового направления юридических исследований // Правоведение. — 2013. — № 2. — С. 93–114.

[2] Батурин Ю. М., Полубинская С. В. Что делает виртуальные преступления реальными // Труды Института государства и права РАН. — 2018. — Т. 13, № 2. — С. 9–35.

[3] Бачило И. Л. Информационное право: учебник. — М.: Норма, 2010. — 816 с.

[4] Габов А. В. Цифровизация и право: сборник научных трудов. — М.: ИГП РАН, 2019. — 320 с.

[5] Талапина Э. В. Персональные данные: от конституционного права к цифровой экономике // Журнал российского права. — 2018. — № 10. — С. 5–19.

[6] Хабриева Т. Я. Право в условиях цифровизации: монография. — М.: Норма, 2020. — 368 с.

[7] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.). С. 3451

[8] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. — 2017. — № 20. — Ст. 2901.

References:

[1] Arkhipov V.V. Virtual law: the main problems of a new direction of legal research//Jurisprudence. — 2013. — № 2. - S. 93-114.

[2] Baturin Yu. M., Polubinskaya S. V. What makes virtual crimes real//Proceedings of the Institute of State and Law of the Russian Academy of Sciences. — 2018. - T. 13, NO. 2. - S. 9-35.

[3] Bachilo I. L. Information law: textbook. - M.: Norma, 2010. - 816 s.

[4] Gabov A.V. Digitalization and law: a collection of scientific works. - M.: IGP RAS, 2019. - 320 s.

[5] Talapina E.V. Personal data: from constitutional law to the digital economy//Journal of Russian Law. — 2018. — № 10. - S. 5-19.

[6] Khabrieva T. Ya. Law in the context of digitalization: monograph. - M.: Norma, 2020. - 368 p.

[7] Federal Law No. 27.07.2006 dated 152-FZ “On Personal Data “//” Collection of Legislation of the Russian Federation,” 31.07.2006, No. 31 (1 part). Page 3451

[8] On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030: Decree of the President of the Russian Federation of 09.05.2017 No. 203//Collection of Legislation of the Russian Federation. — 2017. — № 20. - Art. 2901.

