



Научная статья

УДК 34:004:343.213.3:343.232:343.235.4

EDN: <https://elibrary.ru/rowsaq>

DOI: <https://doi.org/10.21202/jdtl.2025.23>

Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной

Мурад Мамедович Маджумаев

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Ключевые слова

аватар,
виртуальная реальность,
дополненная реальность,
место преступления,
метавселенная,
право,
преступление,
уголовное право,
цифровые технологии,
юрисдикция

Аннотация

Цель: провести критический анализ возможности распространения существующих принципов действия уголовного закона в пространстве на деяния, совершенные в децентрализованных виртуальных мирах метавселенной, и разработать предложения, включающие обновление подхода к установлению юрисдикции в отношении таких виртуальных преступлений.

Методы: методологическую основу исследования составляет совокупность общенаучных методов и подходов научного познания – диалектический, формально-логический (анализ и синтез, индукция и дедукция), системный, а также частно-научные методы – формально-правовой, правовое моделирование, толкование. Исследование опирается на анализ судебной практики, зарубежного законодательства, технических особенностей блокчейн-технологий и децентрализованных автономных организаций, что позволяет выявить пробелы в правовом регулировании и предложить концептуально новые решения для определения места совершения преступления в виртуальной среде.

Результаты: выявлена ограниченность реализации существующих общепринятых принципов определения юрисдикции в отношении виртуальных преступлений, которые не имеют физических координат. Предлагаемая многофакторная модель юрисдикции переопределяет «место преступления» с учетом таких факторов, как цифровая идентичность правонарушителя, характер и местонахождение цифровых активов, протоколы управления платформой и причиненный реальный ущерб. Предполагается, что неизменяемый и верифицируемый характер операций в блокчейне может служить своеобразным юридическим эквивалентом физического присутствия для установления персональной юрисдикции, позволяя инициировать уголовное преследование даже в тех случаях, когда фактическое местонахождение правонарушителя остается неизвестным.

© Маджумаев М. М., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: в работе изложен подход, предполагающий фундаментальное преобразование реактивных, адаптивных принципов правового регулирования в проактивную, комплексную основу, предназначенную специально для уникальных вызовов метавселенной. Выдвинута меняющаяся парадигма гипотеза, которая заключается в том, что постоянный (устойчивый) цифровой след правонарушителя в виртуальных пространствах может служить основой для осуществления юрисдикции. В модели системно увязано представление о вреде как важнейшем звене между виртуальными правонарушениями и их последствиями в реальном мире.

Практическая значимость: обусловлена отсутствием в настоящее время возможности применения к отношениям в метавселенной правовых норм и правил, учитывающих их специфику. Основные положения и выводы исследования могут быть использованы для совершенствования механизмов правового регулирования метавселенной, формирования международных протоколов об обмене данными и взаимной правовой помощи в вопросах поиска и сбора доказательств, основанных на технологии блокчейн, а также для разработки законодательных инициатив, направленных на создание комплексных правовых механизмов, масштабируемых и устойчивых к быстрым технологическим изменениям, характерным для цифровой среды.

Для цитирования

Маджумаев, М. М. (2025). Многофакторная модель юрисдикции: переосмысление места преступления в децентрализованной метавселенной. *Journal of Digital Technologies and Law*, 3(4), 570–597. <https://doi.org/10.21202/jdtl.2025.23>

Содержание

Введение

1. Криминализация метавселенной
2. Принципы действия уголовного закона в пространстве
 - 2.1. Территориальный принцип
 - 2.2. Экстратерриториальное действие уголовного закона
3. Феномен метавселенной: понятие и онтологические свойства
4. Технологическая основа метавселенной
5. Цифровые аватары (цифровые двойники)
6. Действие уголовного закона в метавселенной
7. Многофакторная модель юрисдикции: переосмысление места преступления в метавселенной
 - 7.1. Установление юрисдикции в отношении субъектов виртуального деяния в метавселенной
 - 7.2. Цифровые активы как основание для определения юрисдикции in rem

7.3. Протоколы платформ (управление кодом) как основание для определения юрисдикции

7.4. Вред (физическая связь или конечный результат) как основание для юрисдикции

Заключение

Список литературы

Введение

Становление метавселенной, концептуально представленной как сеть регулируемых, постоянных, иммерсивных, интерактивных и взаимосвязанных виртуальных миров, сочетающих в себе технологии виртуальной (VR), дополненной (AR) и смешанной (MR) реальностей, а также технологии блокчейна, несет в себе серьезный вызов устоявшимся принципам уголовного права, в особенности определению действия закона в пространстве. Исторически государственный суверенитет и неотъемлемое право принимать и применять законы были неразрывно связаны с территориальностью, которая лежит в основе Вестфальской системы международного правопорядка (Chimni, 2022). Из этого основополагающего принципа следует, что юрисдикция государства в отношении действий, совершаемых на его «физической» территории (на суше, в воздушном пространстве, во внутренних водах и территориальном море, на континентальном шельфе и в исключительной экономической зоне), в принципе является законной, в то время как притязания в отношении деяний, совершаемых за пределами его территории, считаются неправомерными (за исключением принципов экстратерриториальности).

При всей своей исторической укорененности подобная традиционная модель (территориальности и общепринятые принципы экстратерриториальности) становится все более «искусственной» в цифровую эпоху. В частности, согласно акторно-сетевой теории, объекты (артефакты, технические комплексы, нечеловеческие «агенты», алгоритмы), так называемые акторы или актанты, воспринимаются как действующие единицы общественных отношений (Wei, 2023). Как представляется, к таким акторам (актантам) можно отнести и цифровых двойников людей в метавселенной, которые в состоянии взаимодействовать и влиять на виртуальную сеть. Основная проблема заключается в фундаментальной несовместимости такой модели юрисдикции, привязанной к физической территории государства, с безграничной, «нефизической» и децентрализованной архитектурой метавселенной. Метавселенная полностью лишена физических координат (Brey, 2025).

В настоящей статье будут использоваться термины *locus delicti*, «место преступления» и «место происшествия». Хотя они не являются тождественными по содержанию, здесь они будут пониматься как имеющие одинаковое значение, за исключением случаев, когда это специально оговорено по-другому. *Locus delicti* (лат. «место преступления») означает местность, в которой имели место признаки объективной стороны состава преступления. Место преступления является более узким и конкретным понятием. Это основное место, где было совершено преступление, независимо от того, где наступили общественно опасные последствия преступления или где обнаружены сведения о преступлении.

С другой стороны, место происшествия – это более широкая категория. Оно обозначает место или территорию, где имеется информация, относящаяся к событию, которое исследуется в уголовно-процессуальном порядке¹. Сюда относится не только конкретное место преступления, но и любое другое место, где обнаружены объективные последствия преступления или иные следы, имеющие криминалистическое значение.

Определение места совершения преступления (*locus delicti*) является одной из фундаментальных задач уголовно-правовой науки, поскольку от него зависит решение ряда принципиальных вопросов. Во-первых, оно определяет право, применимое к конкретному преступлению, а также надлежащую подсудственность и подсудность дела. С этим напрямую связаны сроки давности уголовной ответственности, поскольку их установление зависит от юрисдикции, в которой было совершено преступление. Во-вторых, место совершения преступления служит отправной точкой для установления составообразующих признаков деяния и его правильной квалификации, что, в свою очередь, влияет на реализацию принципа *non bis in idem* («не дважды за одно и то же») и вопросы экстрадиции.

С точки зрения уголовно-процессуального права место совершения преступления является незаменимым ориентиром для почти что всех следственных действий. Оно служит основным источником сбора доказательств, обеспечивая надлежащую цепочку доказывания, от которой зависят их последующая проверка и оценка. В дополнение к этому место преступления является исходной точкой для поиска свидетелей, проверки алиби и мотивировки процессуальных документов, таких как постановления следователя о проведении обыска и выемки (или решение суда, если обыск проводится в жилом помещении). Все эти действия в совокупности способствуют построению дела, которое позволит предъявить обоснованное обвинение с учетом презумпции невиновности.

В криминалистике место преступления – это центральный элемент, определяющий весь процесс расследования. Это крайне важно для проведения осмотра места преступления, построения криминалистических версий событий и планирования дальнейших следственных действий. На месте преступления осуществляется сбор всех видов доказательств, их криминалистическая фото- и видеофиксация. Здесь же организуется взаимодействие следователя (дознателя), сотрудников оперативно-разыскных подразделений, при необходимости – уполномоченных представителей правоохранительных органов других государств. Кроме того, на месте преступления активно работают сведущие лица, обладающие специальными знаниями (специалисты, а впоследствии эксперты при проведении экспертиз), что способствует эффективному раскрытию и расследованию преступлений.

Определение места совершения преступления (*locus delicti*) особенно важно при расследовании преступлений, составообразующие признаки которых полностью или частично сосредоточены в децентрализованном виртуальном пространстве – метавселенной. Так, общий объем оборота мирового рынка метавселенных демонстрирует стремительный рост, который в 2024 г. был оценен в 110,4 млрд долларов США, а к 2034 г., по прогнозам, превысит 4,47 трлн долларов США, отражая высокий

¹ Бертовский, Л. В. (ред.). (2021). Криминалистика: учебник для бакалавров (2-е изд., перераб. и доп.). Москва: РГПРЕСС.

совокупный годовой темп роста (CAGR) на уровне 44,8 %². Наибольший вклад в 2024 г. был внесен в сегмент аппаратного обеспечения, включающий передовые гарнитуры и тактильные датчики, на долю которого пришлось 52,8 % общей доли рынка³. Базовые технологии виртуальной реальности (VR) и дополненной реальности (AR) в совокупности составили 34,2 % рынка, формируя основу иммерсивных цифровых сред⁴.

Пользовательская база метавселенной в основном складывается из молодежи (четыре из пяти пользователей моложе 16 лет) и насчитывает около 700 млн активных пользователей в месяц по всему миру⁵. Прогнозы роста весьма внушительны, некоторые отчеты предполагают, что к 2030 г. число пользователей достигнет 5 млрд, учитывая пользователей мобильных телефонов, в то время как более точные оценки, основанные на данных о пользователях устройств VR/AR, прогнозируют цифру ближе к 1 млрд⁶. Это обуславливает актуальность исследования рассматриваемой проблемы относительно определения *locus delicti* в деяниях, совершенных в метавселенной.

В данной статье рассматривается фундаментальная проблема действия уголовного права в децентрализованной виртуальной среде метавселенной. Прежде всего, анализируется проблема криминализации метавселенной, что является основанием для обсуждения применимости к ней традиционных правовых подходов. Далее подробно разбираются устоявшиеся принципы уголовной юрисдикции в пространстве, в частности территориальный и экстратерриториальный подходы и их ограничения при применении к виртуальной среде. Затем проводится исследование феномена метавселенной, описание ее онтологических свойств, таких как иммерсивность, синхронность, устойчивость, совместимость и децентрализация, а также ее технологических основ и роли цифровых аватаров. Вслед за этим дается критическая оценка действия уголовного закона в метавселенной, которая приводит к основному тезису данной работы: необходимости разработки новой многофакторной модели юрисдикции. Эта модель, призванная переосмыслить концепцию *locus delicti* в метавселенной, систематически определяет юрисдикцию на основе многостороннего анализа цифровой идентичности правонарушителя, местонахождения цифровых активов, протоколов управления платформой, а также фактического ущерба или физической связи, вызванных виртуальным действием.

1. Криминализация метавселенной

Несмотря на то, что часть из приведенных ниже примеров носят гражданско-правовой характер, на их основе можно наметить ориентиры, полезные для переосмысления понятия места происшествия в уголовном праве.

Один из наиболее заметных конфликтов правовых интересов возникает в связи с незаконным использованием интеллектуальной собственности в метавселенной.

² Metaverse Market. Report ID: 101905. (2025). Market.us Scoop. <https://clck.ru/3QGxSF>

³ Там же.

⁴ Там же.

⁵ Duarte, F. (2025, June 5). Number of Metaverse Users in 2025. Exploding Topics. <https://clck.ru/3QGxcm>

⁶ Там же.

Наглядным тому примером является гражданский спор между Roblox Corporation (далее – Roblox) которая разрабатывает и управляет виртуальной онлайн-платформой развлечений, и WowWee Group Limited (далее – WowWee), ведущим разработчиком, производителем, продавцом и дистрибьютором инновационных высокотехнологичных потребительских роботов, развлекательных продуктов и других игровых устройств. Компания Roblox, имеющая регистрацию в Калифорнии (США), утверждала, что компания WowWee, зарегистрированная в Гонконге, незаконно воспроизвела (скопировала) дизайн виртуальных аватаров Roblox для создания и реализации линейки физических фигурок (кукол) под названием My Avastars⁷. Исходя из представленных доказательств, было установлено, что WowWee намеренно стремилась позиционировать эти куклы как «реальные» версии аватаров Roblox, т. е. установить связь между своим физическим продуктом и экосистемой Roblox, тем самым используя виртуальную интеллектуальную собственность для получения материальной выгоды⁸.

В случае уголовного преследования за нарушение авторских и смежных прав данное дело представляет собой многогранную юрисдикционную дилемму, поскольку необходимо определить место совершения преступления (*locus delicti*). Это может быть Гонконг, где физически находится WowWee; Калифорния (США), где находится Roblox; место расположения серверов (облако, диск), где хранятся данные онлайн-платформы Roblox, или децентрализованное виртуальное пространство (метавселенная), где находится оригинальный аватар, защищенный авторским правом.

Аналогичным является спор между Impulse Communications, Inc. (корпорация из Делавэра со штаб-квартирой в Род-Айленде, США) и Uplift Games LLC, Treetop Games LLC, Lionfield Investments LTD – компаниями, которые управляют виртуальными играми с домашними животными под названием Adopt Me⁹.

Еще один схожий случай имел место в споре между Hermès International (Париж, Франция) и Hermès of Paris, Inc. (Нью-Йорк, США) и Мейсоном Ротшильдом (Лос-Анджелес, Калифорния, США). Г-н Ротшильд, действуя из Калифорнии, создал и коммерциализировал коллекцию цифровых активов под названием MetaBirkins в форме невзаимозаменяемых токенов (NFT), которые представляли собой цифровые копии известной сумки Hermès Birkin и продвигались как предметы роскоши в метавселенной¹⁰.

При уголовном преследовании за нарушение прав на товарный знак возникнет такая же серьезная проблема установления конкретного места совершения преступления. При определении юрисдикции местом преступления могут выступать места нахождения Hermès International (Париж, Франция), Hermès of Paris, Inc (Нью-Йорк, США), Мейсона Ротшильда (Калифорния, США) или место нахождения децентрализованной блокчейн-сети, где были созданы и проданы NFT, нарушающие права.

⁷ Roblox Corporation et al v. WowWee Group Limited et al, No. 3:2022cv04476-SI – Document 69 (N.D. Cal. 2024). <https://clck.ru/3QGxeC>

⁸ Там же.

⁹ Impulse Communications, Inc. v. Uplift Games, LLC et al, No. 24-cv-166-JJM-LDA – Document 29 (D.R.I. 2024). <https://clck.ru/3QGxjZ>

¹⁰ Hermes International et al v. Rothschild, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). <https://clck.ru/3QGxnH>

Как следует из обвинительного заключения, в другом случае с 2018 по 2022 г. соучастники вступили в преступный сговор с целью обмана инвесторов группы компаний, принадлежащих одному из злоумышленников¹¹. Они собирали средства под обещание разработки технологий виртуального мира, в том числе собственной криптовалюты, которая должна была использоваться в создаваемой ими метавселенной¹². Они также обещали заведомо недостижимые высокие доходы и распространяли ложные заявления о том, что в приобретении участвуют известные предприниматели и состоятельные покупатели¹³. Вместо этого они незаконно присвоили средства для личной выгоды, в том числе использовали деньги для покупки личных объектов недвижимости¹⁴. Этот случай показывает, что, если бы вся схема была реализована в полностью децентрализованной метавселенной без использования традиционной инфраструктуры, возникли бы проблемы с определением юрисдикции.

Наконец, наиболее яркое проявление рассматриваемой проблемы прослеживается в полицейском расследовании в Великобритании преступления против половой неприкосновенности, совершенного в иммерсивной виртуальной реальности. В результате развратных действий жертва, как утверждается, получила психологическую и эмоциональную травму, которая, несмотря на отсутствие физического контакта, является очевидным признаком объективной стороны состава преступления¹⁵. Возникает актуальный вопрос: где находится место преступления, если оно совершено исключительно с использованием аватаров в виртуальном пространстве? Место преступления может быть определено физическими координатами жертвы или преступника либо виртуальной средой (метатерриторией), на которой было совершено преступление.

Все эти примеры требуют нового правового подхода к определению места преступления, признания метавселенной в качестве полноценного нового пространства для совершения преступлений, что, в свою очередь, требует новых принципов определения действия уголовного закона в пространстве.

2. Принципы действия уголовного закона в пространстве

2.1. Территориальный принцип

Основным началом, определяющим действие уголовного закона в пространстве, является принцип территориальности. В соответствии с этим принципом государство обладает исключительной юрисдикцией по преследованию и наказанию за преступления, совершенные на его территории (Payer, 2023). Преступление считается совершенным на территории Российской Федерации, если любое из его составных признаков, в том числе начало, продолжение или завершение, имело

¹¹ United States District Court District of Nebraska. (2025, June 4). 22-3077 – USA v. Chandran et al. [Government]. Administrative Office of the United States Courts. <https://clck.ru/3QGxrp>

¹² Там же.

¹³ Там же.

¹⁴ Там же.

¹⁵ Camber, R. (2024, January 1). British police probe VIRTUAL rape in metaverse: young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' – sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. <https://clck.ru/3QGxwo>

место в пределах ее государственной границы (доктрина субъективной территориальности, доктрина объективной территориальности и доктрина эффекта (последствий) (Ryngaert, 2023).

Территория Российского государства, определяемая Основным законом Российской Федерации, включает в себя сухопутную территорию, водную территорию, недра и воздушное пространство (ч. 1 ст. 67 Конституции РФ). Сухопутная территория охватывает материковую часть и острова в пределах государственной границы. Водная территория объединяет внутренние воды, такие как реки и озера, а также территориальное море – полосу морской акватории шириной 12 морских миль, примыкающую к суше или внутренним водам (ч. 1 ст. 2 ФЗ «О внутренних морских водах, территориальном море и прилежащей зоне Российской Федерации») ¹⁶. Недра являются частью земной коры под поверхностью земли (почвенного слоя, а при его отсутствии – ниже земной поверхности и дна водоемов и водотоков, простирающейся до глубин, доступных для геологического изучения и освоения) (преамбула ФЗ «О недрах») ¹⁷, а воздушное пространство – это область над сушей и водой с предполагаемым верхним пределом 100–110 км (условная граница между атмосферой Земли и космосом (линия Кармана) (Pogorzelska, 2024).

Государственная граница, определяющая суверенную территорию Российской Федерации, представляет собой вертикальную плоскость, проходящую по этим физическим границам. За пределами этих определенных зон территориальный принцип применяется к определенным преступлениям, совершенным на континентальном шельфе Российской Федерации и в ее исключительной экономической зоне. Обе эти зоны являются морскими районами за пределами территориального моря, где Российская Федерация осуществляет особые суверенные права, в частности в отношении природных ресурсов.

Российский уголовный закон, согласно территориальному принципу, распространяется на преступления, совершенные на гражданских морских и воздушных судах, зарегистрированных в Российской Федерации, когда они находятся в международных водах или воздушном пространстве, а также на российских военных морских и воздушных судах независимо от их местонахождения (ч. 3 ст. 11 УК РФ) ¹⁸.

2.2. Экстратерриториальное действие уголовного закона

Принято выделять случаи, в которых предполагается осуществление юрисдикции государства за пределами его национальных границ, известной как экстратерриториальная юрисдикция. В этой связи различают следующие принципы: активного гражданства, пассивного гражданства, защитного и универсальной юрисдикции.

Принцип активного гражданства (персонального, национального) отражает право государства осуществлять уголовную юрисдикцию в отношении своих граждан,

¹⁶ О внутренних морских водах, территориальном море и прилежащей зоне Российской Федерации. № 155-ФЗ от 31 июля 1998 г. (с изм. и доп., Федеральным законом от 31 июля 2025 г. № 304-ФЗ). Гарант. <https://clck.ru/3QGyAr>

¹⁷ О недрах. № 2395-1 от 21 февраля 1992 г. (с изм. и доп., Федеральным законом от 31 июля 2025 г. № 353-ФЗ). КонсультантПлюс. <https://clck.ru/3QGyCQ>

¹⁸ Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. КонсультантПлюс. <https://clck.ru/3QGyDx>

совершивших уголовно наказуемые деяния за пределами его территории, независимо от их географического местонахождения (Есаков, 2015).

С другой стороны, хотя это и является предметом научных дискуссий, принцип пассивного гражданства (пассивное персональное) подразумевает осуществление экстратерриториальной уголовной юрисдикции государством в отношении преступлений, где жертвой является его гражданин (Есаков, 2015). В этом случае преступление совершается иностранными подданными (или лицами без гражданства) за пределами государственной границы.

В случае если преступлением, совершенным вне территории государства иностранным гражданином (или лицом без гражданства), посягают на интересы этого государства, то в соответствии с принципом защиты применяется право этого государства (Есаков, 2015).

Принцип универсальности допускает применение права государства при уголовном преследовании иностранных граждан и лиц без гражданства, совершивших преступления против мира и безопасности человечества. Применение данного принципа является оправданным ввиду соображений международной публичной политики (Есаков, 2015).

3. Феномен метавселенной: понятие и онтологические свойства

Концепция метавселенной, некогда ограничивавшаяся сферой научной фантастики, в настоящее время превращается в новую реальность, которая в перспективе даст новое выражение человеческому взаимодействию в цифровом измерении. В 1992 г. Нил Стивенсон в своем романе «Лавина» описал метавселенную как виртуальную реальность, которая заменит Интернет (Ioannidis & Kontis, 2023). С тех пор идея метавселенной значительно усовершенствовалась с развитием виртуальной реальности (VR), дополненной реальности (AR), тактильных технологий (haptics) и технологий искусственного интеллекта.

Метавселенная – это совокупность взаимосвязанных цифровых пространств и явлений, объединяющих виртуально усиленную физическую реальность и физически устойчивую виртуальную реальность. Таким образом, происходит качественный переход от нынешней стадии развития сети Интернет к иммерсивной трехмерной онлайн-среде. Сетевое пространство, предлагаемое в рамках концепции метавселенной, позволяет пользователям взаимодействовать друг с другом и с компьютерной средой в режиме реального времени, как правило, с помощью цифровых аватаров (Han et al., 2023). Его преобразующий потенциал распространяется практически на все сферы человеческой жизнедеятельности, включая здравоохранение, образование, трудовую деятельность, социальное взаимодействие, торговлю и развлечения.

Иммерсивность

Характерной чертой метавселенной является ее способность погружать пользователей в трехмерное пространство. Это погружение достигается с помощью передовых устройств расширенной реальности (XR), которые включают в себя гарнитуры виртуальной реальности (VR), устройства дополненной реальности (AR) и технологии смешанной реальности (MR). Эти инструменты используют стереоскопические изображения и пространственный звук для создания иллюзии глубины и пространства, позволяя пользователям чувствовать себя «реальными» (телеприсутствие) в месте, отличном от их физического местоположения (Bhowmik, 2024). Степень сенсорного погружения играет решающую роль в пробуждении эмоций и влиянии на поведение

пользователей. Такой глубокий уровень вовлеченности означает, что виртуальные впечатления могут оказывать значительное психологическое воздействие, еще больше стирая грань между виртуальным и реальным мирами.

Синхронность взаимодействия

Метавселенная обеспечивает взаимодействие между пользователями и виртуальной средой в режиме реального времени (Hosseini et al., 2024). Такая мгновенность имеет решающее значение для создания динамичного и оперативного опыта, позволяя осуществлять синхронное социальное взаимодействие, совместную работу и гибкий игровой процесс. Ощущение «присутствия» в значительной степени усиливается благодаря мгновенной адаптации обзора пользователя и сенсорной обратной связи в ответ на его движения и действия (Hosseini et al., 2024). Эта реальность означает, что действия и их последствия в метавселенной могут быть моментальными.

Устойчивость (постоянство)

Следующая особенность метавселенной – ее постоянство, которое обеспечивает непрерывное существование виртуального мира и всех происходящих в нем изменений, даже когда пользователи не подключены к системе (Richter & Richter, 2023). Это означает, что аватары пользователей, цифровые двойники (виртуальные представления объектов) и состояние пространств метавселенной остаются неизменными во времени, обеспечивая устойчивость и целостность. В отличие от традиционных онлайн-игр, где сессии заканчиваются, а прогресс может быть сброшен или ограничен конкретными эпизодами, по-настоящему постоянная метавселенная подразумевает стабильную цифровую среду, которая развивается на основе действий пользователей и остается неизменной, пока сами пользователи не изменят ее. Хотя современные платформы демонстрируют определенную степень локальной персистентности, общий критерий стабильного, универсального постоянства, каким его представляют для метавселенной, остается важной областью для технологического прогресса и исследований.

Интероперабельность

Другим свойством метавселенной считается функциональная совместимость (интероперабельность), которая заключается в возможности бесшовного перемещения виртуальных цифровых объектов, аватаров и данных между различными виртуальными мирами и платформами в пределах всей метавселенной (Richter & Richter, 2023). Именно это свойство обеспечивает единство и взаимосвязанность цифровой вселенной, что значительно отличается от текущего состояния, когда виртуальные миры в значительной степени несовместимы друг с другом и часто остаются «закрытыми». Общеизвестно, что для обеспечения подлинной интероперабельности необходимы совместимые технологии, оборудование, протоколы и стандарты, которые обеспечивают беспрепятственный обмен информацией и одновременное реагирование различных систем.

Децентрализованность

Главной особенностью метавселенной выступает ее децентрализованность, предполагающая распределение контроля и прав между участниками сети (McStay, 2023), а не их концентрацию в руках одного центрального органа (провайдера). Фактически это неотъемлемый принцип управления метавселенной, влияющий на принятие решений, установление правил и поддержание общей структуры виртуальной среды. Основным инструментом децентрализации является технология блокчейн, которая обеспечивает прозрачность и автономность путем записи

транзакций и изменений в общедоступном и неизменяемом реестре (Panda, 2023). Такой распределенный контроль направлен на расширение прав пользователей, предоставляя им больше прав на свои цифровые активы (такие как виртуальная недвижимость, предметы в играх и виртуальная валюта) и прямое участие в принятии управленческих решений, что снижает уязвимость перед произвольными действиями центрального органа. Децентрализация также способствует преодолению цензуры, поскольку ни одна организация не в состоянии предписывать содержание или ограничивать доступ, а это способствует свободе самовыражения и творчеству.

4. Технологическая основа метавселенной

Функционирование метавселенной основано на синергетической интеграции различных передовых технологий, образующих многоуровневую экосистему, которая поддерживает ее иммерсивные, постоянные и интерактивные характеристики.

Расширенная реальность (XR) – это общий термин, который охватывает виртуальную реальность (VR), дополненную реальность (AR) и смешанную реальность (MR) и представляет собой спектр иммерсивных технологий, используемых для доступа к метавселенной и взаимодействия с (в) ней (Özkan & Özkan, 2024).

Виртуальная реальность (VR) погружает пользователей в полностью компьютерную, искусственную трехмерную среду. Обычно это достигается с помощью шлемов виртуальной реальности, которые оснащены стереоскопическими экранами и пространственным звуком, создавая сильное ощущение присутствия (Bhowmik, 2024). Датчики движения отслеживают движения пользователя, корректируя виртуальный обзор в режиме реального времени, а устройства тактильной обратной связи могут создавать ощущение прикосновения, позволяя пользователям манипулировать виртуальными объектами (Bhowmik, 2024).

Дополненная реальность (AR) накладывает на физический мир цифровые данные (элементы, объекты), улучшая восприятие реальности пользователем (Bhowmik, 2024). В отличие от VR, AR сочетает физические и цифровые элементы, создавая целостный интерфейс, который интегрирует виртуальный контент в реальное окружение пользователя, часто с помощью таких устройств, как смартфоны или прозрачные модули головного шлема VR. С помощью приложений AR пользователи могут взаимодействовать с отображаемыми данными, как если бы они были реальными, получать доступ к картам или создавать общие AR-опыты (Syed et al., 2022).

Смешанная реальность (MR) сочетает в себе элементы VR и AR, позволяя цифровым и реальным объектам сосуществовать и взаимодействовать в режиме реального времени (Rokhsaritalemi et al., 2020). Эта технология представляет собой более продвинутую форму смешения физической и виртуальной реальности.

5. Цифровые аватары (цифровые двойники)

В метавселенной пользователи используют виртуальных аватаров в качестве своих цифровых представлений, посредством которых они выражают себя, коммуницируют и иным образом взаимодействуют с другими в виртуальном пространстве (Kim et al., 2025). Эти аватары могут быть в значительной степени настраиваемыми, что позволяет пользователям выражать себя уникальными способами или даже воссоздавать персонажей из популярной культуры. Возможность создавать и воплощать цифровые идентичности выходит за рамки простых профильных фотографий, представляя индивидуальность, стиль и даже социальный статус в метавселенной.

При этом сама концепция цифровой личности в метавселенной остается сложной и многогранной, принципиально отличающейся от личности в реальном мире. В цифровом пространстве один человек может иметь несколько различных и даже псевдонимных личностей, что усложняет традиционные представления об удостоверении личности и ответственности. Все большее сближение реальных и виртуальных личностей означает, что вред, нанесенный аватару пользователя, может иметь серьезные моральные и правовые последствия в реальном мире. Разумеется, при таком понимании цифровой личности возникают новые правовые вопросы, касающиеся личных прав, мошенничества и введения в заблуждение в виртуальной среде.

6. Действие уголовного закона в метавселенной

В основном традиционные правовые предписания сосредоточены на общественных отношениях в физическом мире, складывающихся между людьми, находящимися на определенной территории. Метавселенная по своей природе преодолевает подобные физические границы, создавая глобальное, взаимосвязанное цифровое пространство, в котором пользователи из разных стран могут легко взаимодействовать друг с другом. Это принципиальное новое обстоятельство означает, что действия, совершаемые в виртуальном мире, могут иметь последствия в реальном мире в нескольких юрисдикциях, как свидетельствуют приведенные выше примеры. Следовательно, становится гораздо сложнее определить, законодательство какой страны подлежит применению, а также установить подследственность и подсудность уголовного дела.

Как принято считать, Web 3 – следующий этап развития Интернета – ставит новые задачи в плане учета геополитических границ, однако многие виды онлайн-деятельности по-прежнему косвенно привязаны к местоположению пользователя через такие параметры, как язык, часовой пояс, доменные имена, IP-адреса и другие метаданные. Возможно, наиболее важным и в то же время чреватым определенными рисками является то, что погружение в виртуальный мир, особенно в тот, который призван имитировать или (условно) заменить реальный мир, не подразумевает презумпцию обязательного подчинения законам какой-либо конкретной страны за исключением, возможно, правил данной платформы (метавселенной).

Ограниченность существующих принципов определения юрисдикции и правовых конструкций в части надлежащего реагирования на своеобразные вызовы метавселенной свидетельствует о необходимости выработки новых всеобъемлющих правовых подходов. Реактивный подход, сводящийся к попыткам просто адаптировать существующие правовые нормы к новым цифровым реалиям, может оказаться недостаточным и повлечь за собой постоянное появление пробелов в правовом регулировании, особенно в уголовно-правовом.

7. Многофакторная модель юрисдикции: переосмысление места преступления в метавселенной

На основании изложенного предлагается пересмотреть содержание понятия «место преступления» в децентрализованной метавселенной и рассматривать его не как определенную пространственную точку, а как распределенную систему отдельных компонентов. В данной системе каждый компонент (признаки преступного деяния как внутри метавселенной, так и за ее пределами) является самостоятельным

звенем, определяющим юрисдикцию. Представляется целесообразным определять юрисдикцию на основе комплексного анализа всех этих компонентов, не ограничиваясь одним, зачастую условным, местоположением в физическом пространстве.

Основная идея модели многофакторной юрисдикции заключается в рассмотрении преступления как события, имеющего несколько юридически значимых точек соприкосновения в цифровом и физическом пространстве, нежели как деяния, совершенного в одном конкретном географическом месте. Элементы этой модели основаны на теоретическом осмыслении устоявшихся правовых принципов определения действия уголовного закона в пространстве и призваны обеспечить структурированную и надежную основу для осуществления уголовного преследования.

Предлагаемая модель включает четыре ключевых фактора, каждый из которых предоставляет суду отдельное основание для определения уголовной юрисдикции:

- а) субъект (виртуального деяния);
- б) цифровые активы;
- в) протоколы платформы (управление кодом);
- г) вред (физическая связь или конечный результат).

7.1. Установление юрисдикции в отношении субъектов виртуального деяния в метавселенной

Установление личности лица, совершившего преступления в метавселенной, следует осуществлять на основе информации, содержащейся в распределенном реестре (иными словами, в блоках, связанных между собой в цепочку в децентрализованной базе данных (блокчейне) (Komalavalli et al., 2020), либо посредством псевдонима, ассоциированного с цифровой личностью правонарушителя. В данном случае фиксируется неизменный и необратимый цифровой след преступной деятельности.

Главной отличительной особенностью виртуального действия является его неизменяемость. После фиксации оно навсегда записывается в распределенный реестр (блокчейн), что и делает его неизменяемым и необратимым (Aakula et al., 2023). Каждый блок содержит криптографические ссылки на предыдущий блок, временную метку и данные о транзакции, что технически исключает возможность изменения информации в отдельном блоке без изменения всей цепочки (Aakula et al., 2023). Этот механизм обеспечивает исключительно надежный и поддающийся проверке цифровой след деятельности, который может послужить достоверным доказательством.

Распределенная природа записи действия означает, что информация распространяется по сети взаимосвязанных узлов, а не хранится в едином централизованном репозитории (Aakula et al., 2023). Таким образом достигается повышение прозрачности, устойчивости к подделке и глобальной доступности записей. Примерами виртуальных деяний могут служить передача цифровых активов, использование вредоносных смарт-контрактов (например, при совершении хищений) или даже виртуальное преследование. Эти действия, хотя и происходят исключительно в виртуальной среде, имеют ощутимые правовые и экономические последствия в реальном мире.

Основная гипотеза заключается в том, что адрес правонарушителя в блокчейне, в силу своей верифицируемой, неизменяемой и отслеживаемой активности, приобретает своеобразный юридический эквивалент физического присутствия для целей установления персональной юрисдикции. В этом состоит принципиальный сдвиг парадигмы, устанавливающий новую форму юрисдикции, основанную на устойчивых

цифровых данных, не ограничиваясь временным физическим местоположением. Столь понятийный сдвиг способствует инициированию уголовного преследования на основании проверяемых и необратимых действий правонарушителя в блокчейне, даже если его физическое местонахождение остается неизвестным. Это согласуется с принципами надлежащего судебного разбирательства, устанавливая четкую, выведенную из цифровых данных связь между уникальным цифровым идентификатором подозреваемого и предполагаемым правонарушением.

Преодоление «парадокса блокчейна» проявляется внутренним противоречием: хотя транзакции в блокчейне могут казаться анонимными из-за использования псевдонимных цифровых кошельков, основная активность в принципе поддается отслеживанию. Подлинная личность правонарушителя может оставаться неизвестной, но его цифровая активность в распределенном реестре постоянно записывается и может быть отслежена с помощью схем подписей и криптографических хэшей, раскрывающих поведенческие паттерны (Trozze et al., 2022). Основная задача заключается в преодолении этого разрыва между отслеживаемой цифровой активностью и реальной личностью.

Если виртуальное действие представляет собой неизменяемую и поддающуюся проверке запись, то само действие становится «осязаемым», поддающимся проверке объектом в цифровом пространстве. Это превращает виртуальное действие из простого доказательства поведения человека в цифровой объект, который может быть предметом исследования в ходе судебного разбирательства. Речь идет не только о том, кто совершил деяние, но и о том, что это деяние представляет собой и где оно зафиксировано (в нашем случае в блокчейне). Это расширяет концепцию предметной юрисдикции (*jurisdiction in rem*) за пределы цифровых активов, распространяя ее на сами цифровые действия. Это означает, что суд может распространить свою юрисдикцию в отношении виртуального действия как отдельной юридической фикции (цифровой «вещи» или «события»), что позволит проводить расследования, выносить судебные запреты (например, блокировать функции смарт-контрактов) или «изымать» цифровой след, даже до того, как правонарушитель будет идентифицирован или физически обнаружен. Это представляет собой значительное расширение принципов *in rem* на сферу цифрового поведения, предоставляя мощный новый инструмент для правоохранительных органов в децентрализованных средах.

Для реализации вышеизложенного, возможно, потребуется разработать и внедрить специальный регламент, предписывающий централизованным биржам и другим сервисам хранить информацию о своих клиентах и предоставлять ее по соответствующему официальному запросу.

Сюда входят сбор и проверка личной информации, включая полное имя, дату рождения, адрес проживания и удостоверение личности установленного образца. Введение такого стандарта на международном уровне позволило бы закрепить за биржами по всему миру обязанность хранить такие данные и предоставлять их по законному запросу, тем самым установив важную связь между адресом в блокчейне и реальным человеком. Тем самым значительно расширились бы возможности правоохранительных органов в преодолении парадокса блокчейна за счет обеспечения законного доступа к идентификационным данным.

Следует, однако, отметить, что существование децентрализованных бирж (DEX), которые зачастую не осуществляют сбор указанных сведений, представляют собой проблему, требующую отдельного научного исследования.

7.2. Цифровые активы как основание для определения юрисдикции *in rem*

Цифровые активы, включая криптовалюты, невзаимозаменяемые токены (NFT) и внутриигровые (компьютерные) объекты, как правило, признаются отдельным видом имущества (или, точнее, права), которые могут быть использованы в преступной деятельности в качестве предмета или средства преступления. Их официальная классификация как новой формы имущества позволяет непосредственно распространить на них действие устоявшегося принципа предметной юрисдикции. Этот принцип предоставляет возможность осуществлять юрисдикцию в отношении спорного имущества, находящегося в пределах территориальной юрисдикции, независимо от физического местонахождения его владельца (Niesel, 2023). Такая правовая классификация имеет решающее значение, поскольку она позволяет осуществлять наложение ареста на имущество и при необходимости его конфискации, являющиеся предметом (средством) преступной деятельности, гарантируя тем самым возможность обращения к правовой защите и возврату имущества в цифровой сфере.

Хотя блокчейн сам по себе служит основным местом нахождения цифровых активов (а фактически сервера хранения), их практическое цифровое местонахождение может быть выведено из ряда обстоятельств. Юрисдикция может быть фактически установлена там, где цифровой актив взаимодействует с физическим миром. Ярким примером служит ситуация, когда цифровые активы были приобретены или отчуждены с использованием фиатной валюты через местное банковское учреждение, что создает четкую и неоспоримую связь с конкретной физической территорией.

Централизованные платформы, такие как биржи, в этом случае выполняют важнейшую функцию и выступают в качестве точек входа (и выхода) из метавселенной в реальный мир. Юрисдикция суда по месту их нахождения распространяется на деятельность этих бирж, что позволяет наложить арест или заморозить активы, хранящиеся на счетах этих платформ.

Альтернативным вариантом установления юрисдикции может стать местонахождение хостинг-провайдера, на сервере которого располагается определенный сегмент децентрализованной сети. Этот подход основан на идентификации и использовании физической инфраструктуры сети Интернет (кабелей, серверов, центров обработки данных), которая лежит в основе даже самых децентрализованных цифровых операций. При юридическом анализе нематериальных активов часто создается юридическая фикция, чтобы привязать эти активы к конкретному месту, с учетом таких факторов, как эффективность правоприменения и доступ к средствам правовой защиты (Wendehorst, 2023). В некоторых случаях это может подразумевать физическое местонахождение цифрового кошелька, если его можно надежно привязать к конкретному лицу.

Вышеупомянутые подходы к определению местоположения активов демонстрируют решающую, часто упускаемую из виду зависимость между централизованными шлюзами и децентрализованными сетями для целей правоприменения. Централизованные биржи по своей природе предоставляют регулируемую «точку контроля», где реальная личность и физическое местоположение могут быть связаны с цифровыми активами в соответствии с требованиями законодательства о противодействии отмыванию денег и финансированию терроризма (Schuler et al., 2024). Однако чисто децентрализованные активы или транзакции, хотя и более сложны для непосредственного изъятия, все же зависят от базовой физической инфраструктуры (узлов, серверов, хостинг-провайдеров) для своей работы (Schuler et al., 2024; Bains et al., 2022).

Все это указывает на необходимость двойного регулирования: для цифровых активов, взаимодействующих с традиционной финансовой системой или централизованными поставщиками услуг, использование этих централизованных структур имеет первостепенное значение для эффективных юридически значимых мер. Для действительно децентрализованных активов, обходящих такие шлюзы, акцент смещается на выявление и утверждение юрисдикции над физической инфраструктурой, поддерживающей сеть. Это подчеркивает фундаментальное противоречие между децентрализованным идеалом метавселенной и практической реальностью правоприменения, подразумевая, что даже самые «безграничные» цифровые активы в конечном итоге привязаны к физической реальности в той или иной степени, будь то через взаимодействие человека с централизованными услугами или через базовую вычислительную инфраструктуру.

7.3. Протоколы платформ (управление кодом) как основание для определения юрисдикции

В части установления юрисдикции под протоколом понимается базовая блокчейн-сеть или набор правил (код), регулирующих виртуальное пространство, в котором было совершено правонарушение. Он представляет собой техническую основу и автоматизированные правила, встроенные в систему. Децентрализованная автономная организация (далее – ДАО), напротив, представляет собой форму управления этим виртуальным пространством, часто построенную на основе конкретного протокола или взаимодействующую с ним (Qin et al., 2022). Она функционирует как организационная структура, обычно управляемая децентрализованными компьютерными программами, с голосованием и финансами, обрабатываемыми через блокчейн (Qin et al., 2022). Правонарушение может быть совершено как посредством использования протокола (например, развертывание вредоносного смарт-контракта), так и внутри ДАО (например, путем фальсификации голосования в ее системе управления).

Принцип «управление кодом» как основа юрисдикции опирается на правовую теорию, согласно которой ДАО по своей природе как самоуправляемая и саморегулируемая структура, может быть вовлечена в преступную деятельность, такую как отмывание (легализация) преступных доходов (Benson et al., 2024) или мошенничество (Scharfman, 2024) (через своих представителей или коллективные действия держателей токенов, либо третьих лиц). Можно провести аналогию с традиционными юридическими лицами, такими как коммерческие организации или государственные структуры. Подобно тому, как коммерческая организация является юридическим лицом, способным нести юридическую (административную, гражданскую) ответственность за свои действия, ДАО, благодаря управлению на основе кода и коллективному принятию решений, может быть признано юридическим лицом в определенных юрисдикциях. «Правило кода» (Judge et al., 2025), которое регулирует операции и транзакции в блокчейне, обеспечивает форму ответственности в цепочке.

Юрисдикция может быть распространена в отношении лиц, которые создали, развернули или активно контролируют протокол, при условии, что они физически находятся в пределах юрисдикции соответствующего государства. Таким образом, применяется традиционная персональная юрисдикция, когда существует связь с человеком, что обеспечивает прямой контакт для правоприменения.

Формальные правовые структуры преобразуют децентрализованный протокол или ДАО из «серой» или двусмысленной сети в юридически признанную организацию с определенным местонахождением и правосубъектностью (Pesqueira, 2025). Это имеет решающее значение во избежание неоднозначных квалификаций деяния, которые могут привести к неограниченной личной ответственности отдельных держателей токенов, что может сдерживать участие в деятельности организации. Обращаясь к зарубежному опыту, можно отметить, что некоторые штаты США (например, Вайоминг¹⁹, Вермонт²⁰, Теннесси²¹ и Республика Маршалловы Острова²²) приняли законы, признающие ДАО в качестве юридических лиц, как правило, в форме децентрализованной автономной организации с ограниченной ответственностью (ДАО ООО). Такое юридическое признание обеспечивает предсказуемость, ограниченную ответственность участников (аналогично традиционным ООО) и возможность ДАО вступать в гражданско-правовые отношения, т. е. заключать договоры, владеть имуществом и взаимодействовать с традиционными правовыми системами.

Вместе с тем присущий ДАО глобальный и децентрализованный характер означает, что они могут затрагивать общественные отношения, возникающие на территориях разных юрисдикций.

Поэтому существует противоречие между идеалом децентрализации и необходимостью обеспечения правовой ответственности. Если децентрализация подразумевает распределение контроля и устойчивость к центральной власти, то предлагаемое решение по юрисдикции над протоколами и ДАО в значительной степени опирается на создание формальных правовых структур и правового статуса для ДАО (как это было сделано в ряде штатов США, упомянутых выше). В этом и видится прямое концептуальное противоречие. Суть децентрализации заключается в устранении единых точек контроля и власти, что по своей природе затрудняет традиционным правовым системам определение ответственной стороны. Навязывание юридической «оболочки» или требование регистрации в качестве ООО, по сути, вновь вводит определенную степень централизации или идентифицируемую правосубъектность. Будучи необходимым для установления юридической ответственности, это может быть воспринято как компромисс с основными принципами децентрализации, но и сдерживать инновации в этой сфере.

Главная задача состоит в достижении прагматичного баланса, при котором можно реализовать юридическую ответственность без ущерба для фундаментальных преимуществ децентрализации, таких как свобода от цензуры и раскрытие новаторских инициатив. Это предполагает будущую правовую среду, в которой все

¹⁹ WY Stat § 17-31-101 (2024). 2024 Wyoming Statutes, Title 17 – Corporations, Partnerships and Associations, Chapter 31 – Decentralized Autonomous Organization Supplement, Article 1 – Provisions, Section 17-31-101 – Short Title. <https://clck.ru/3QGyrv>

²⁰ 11 VT Stats § 4171. 2024 Vermont Statutes, Title 11 – Corporations, Partnerships and Associations, Chapter 25 – Limited Liability Companies, § 4171. Definitions. <https://clck.ru/3QUdkt>

²¹ TN Code § 48-250-101 (2024). 2024 Tennessee Code, Title 48– Corporations and Associations (§ 48-1-101 – 48-250-115) Limited Liability Companies (§ 48-201-101 – 48-250-115), Chapter 250 – Blockchains (§§ 48-250-101 – 48-250-115), Section 48-250-101 – Chapter definitions. <https://clck.ru/3QwuTB>

²² 52 MIRC Ch. 7 § 701. Republic of the Marshall Islands Code, Title 52 – Associations Law, Chapter 7 – Decentralized Autonomous Organization Act 2022. <https://clck.ru/3QwuHz>

больше будут преобладать гибридные правовые структуры, сочетающие аспекты децентрализованного управления с традиционной правосубъектностью.

7.4. Вред (физическая связь или конечный результат) как основание для юрисдикции

Вред (физическая связь или конечный результат) является единственным физически детерминированным элементом модели многофакторной юрисдикции. Он выступает в качестве важнейшей связи с реальным миром, которая связывает виртуальное правонарушение с его материальными, имеющими юридическое значение последствиями для физического лица или организации. Этот фактор непосредственно вписывается и расширяет существующую правовую доктрину последствий, согласно которой юрисдикция может быть установлена на основании негативных последствий деяния, произошедших на определенной территории. Его основная цель – обеспечить доступ жертвы к правосудию в суде по месту своего нахождения, предоставив понятный и доступный путь для возмещения ущерба независимо от виртуальной природы первоначального деяния.

Фактор вреда служит важной отправной точкой для установления юрисдикции в случаях, когда другие факторы (например, личность преступника, конкретное местонахождение цифровых активов) могут быть неоднозначными или недоступными. Он преобразует абстрактный характер преступлений в метавселенной в конкретные правовые конструкции, которые соответствуют существующим, устоявшимся правовым нормам. Помимо этого, этот фактор предполагает, что потерпевшие не останутся без правовой защиты только потому, что преступление было совершено в новой цифровой среде, а значит, будет соблюден основополагающий принцип доступа к правосудию. Конечно, это также означает, что в судебных разбирательствах, связанных с преступлениями в метавселенной, первостепенное значение будет иметь доказательство четкой и прямой причинно-следственной связи между виртуальным действием и реальным ущербом.

В настоящем исследовании выделены лишь психологический вред, ущерб репутации и материальный ущерб как примеры вреда от метапреступлений.

Психологический вред является очевидным и широко распространенным видом вреда, который может быть причинен в виртуальной среде. Опыт виртуальных реальностей, особенно иммерсивных, создаваемых с помощью технологий виртуальной и дополненной реальности (VR/AR), может вызывать подлинные психологические и эмоциональные реакции, делая вред, пережитый в виртуальном пространстве, таким же реальным и значительным, как вред, причиненный в физической среде. Ярким примером является расследование полиции в Великобритании по делу о развратных действиях, совершенных в иммерсивной виртуальной реальности, в ходе которого, по сообщениям, жертва получила «психологическую и эмоциональную травму», несмотря на отсутствие физического контакта²³.

²³ Camber, R. (2024). British police probe VIRTUAL rape in metaverse: young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game' – sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online. <https://clck.ru/3QGzVQ>

Репутационный ущерб, нанесенный в метавселенной, например, распространение ложной информации о бренде, несанкционированное использование товарных знаков на виртуальных товарах или продажа контрафактных виртуальных предметов может привести к значительному и измеримому ущербу репутации и финансовому положению компании или физического лица в реальном мире. Дело *Hermès против Ротшильда* служит наглядной иллюстрацией, когда создание и коммерциализация NFT *MetaBirkins* были признаны нарушением и размыванием прав на товарный знак, что нанесло репутационный и финансовый ущерб *Hermès*²⁴.

Материальный ущерб, помимо прямого финансового ущерба, охватывает вред, нанесенный «цифровому двойнику» реального объекта, что, в свою очередь, приводит к повреждению самого физического объекта. Цифровые двойники – это виртуальные представления физических объектов, процессов или систем, которые динамически имитируют и предсказывают поведение своих (настоящих) физических прообразов (Segovia & Garcia-Alfaro, 2022). Они интегрированы с данными в реальном времени (Segovia & Garcia-Alfaro, 2022), что означает, что злонамеренные действия или уязвимости, используемые в цифровом двойнике, могут непосредственно проявляться в виде повреждения или сбоя в физическом двойнике. В этом контексте признанным риском является использование киберфизических систем.

Природа этих форм вреда – нематериальная, опосредованная цифровыми средствами или связанная со сложными взаимодействиями цифровых двойников – создает значительные и неизбежные сложности с доказыванием. Документирование психологического вреда от виртуального деяния требует преодоления традиционного скептицизма в отношении виртуальной природы вреда, который считается менее реальным, что обуславливает необходимость в надежных психологических и медицинских методах доказывания. Репутационный ущерб, хотя и имеет осязаемые последствия, часто носит рассеянный характер, его трудно точно количественно оценить, и он может быстро распространяться в цифровом пространстве. Материальный ущерб, нанесенный цифровым двойникам, требует высокоспециализированного судебного компьютерно-технического анализа для установления точной причинно-следственной связи между цифровой атакой и физическими последствиями. В этих случаях дело не ограничивается «классическими» вещественными доказательствами.

Все это свидетельствует о значительном и растущем спросе на специализированные судебные экспертизы (например, цифровые психологи, эксперты по оценке брендов, судебные аналитики киберфизических систем) и на разработку новых правовых стандартов для цифровых доказательств. Следует адаптировать правила доказывания для учета и оценки новых форм доказательств, связанных с нематериальным и опосредованным цифровыми технологиями ущербом.

Заключение

Развитие виртуальных миров, метавселенной с присущими им свойствами децентрализации, устойчивости и иммерсивности основательно затрудняет применение традиционных принципов определения действия уголовного закона в пространстве.

²⁴ *Hermès International et al v. Rothschild*, No. 1:2022cv00384 – Document 140 (S.D.N.Y. 2023). <https://clck.ru/3QGzYA>

Устоявшиеся правовые подходы, обусловленные физическими границами (территорией) государства и взаимодействием лиц в объективной действительности, оказываются несостоятельными в отношении преступлений, совершаемых в виртуальных пространствах, не имеющих определенных границ. Приведенные в настоящей работе дела – от нарушений прав интеллектуальной собственности до преступлений собственности и преступлений против половой неприкосновенности – подтверждают наличие серьезного пробела в современном уголовном праве в части определения места совершения преступления в метавселенной.

В целях преодоления этого углубляющегося юрисдикционного пробела в настоящей статье предлагается многофакторная модель юрисдикции, в которой место совершения преступления рассматривается не как конкретная точка в пространстве, а как распределенная система, состоящая из отдельных компонентов. Этот парадигмальный сдвиг, основанный на анализе цифровой идентичности правонарушителя, характера и местонахождения цифровых активов, протоколов управления, встроенных в код платформы, и причиненного материального ущерба, позволяет создать комплексную основу для определения юрисдикции по уголовным делам.

В частности, в модели обосновывается, что неизменяемая и верифицируемая природа блокчейн-транзакций может служить правовым эквивалентом физического присутствия для установления персональной юрисдикции. Кроме того, классификация цифровых активов как самостоятельной формы имущества позволяет напрямую применять юрисдикцию *in rem*, в то время как принцип «управления кодом» способствует установлению юрисдикции в отношении организаций или физических лиц, ответственных за разработку и контроль протоколов. При этом фактор вреда обеспечивает доступ жертв к правосудию, связывая виртуальные правонарушения с их материальными последствиями в физическом мире.

При всей своей теоретической убедительности и целесообразности, предлагаемая модель не лишена внутренних ограничений, заставляющих критически оценить ее. Установление юрисдикции на основе цифровой личности правонарушителя, хотя и теоретически обоснованно, в значительной степени зависит от преодоления «парадокса блокчейна» – внутреннего противоречия между анонимностью псевдонимных цифровых кошельков и отслеживаемостью базовой активности. Работоспособность этого подхода зависит от разработки и внедрения на международном уровне строгих правил для централизованных бирж и создания в будущем механизмов установления личности лиц, стоящих за децентрализованными идентификационными данными. Проблема, создаваемая абсолютно децентрализованными биржами (DEX), которые часто обходят такие меры по сбору данных, остается серьезным препятствием, требующим дальнейшего научного исследования и нормативно-правового регулирования.

Аналогичным образом, хотя классификация цифровых активов в качестве имущества упрощает применение юрисдикции *in rem*, практические механизмы правоприменения в отношении активов, находящихся исключительно в децентрализованных сетях, без взаимодействия с централизованными шлюзами, остаются недостаточно разработанными. Зависимость от идентификации физической инфраструктуры сети Интернет (например, хостинг-провайдеров) для установления юрисдикции над чисто децентрализованными активами, хотя и является необходимой, представляет собой концептуальное противоречие с самой сущностью децентрализации.

Принцип «управления кодом» как юрисдикционной связи также представляет собой смысловую дилемму. Предложение о предоставлении формальных правовых структур и статуса децентрализованным автономным организациям, будучи крайне важным для обеспечения неотвратимости ответственности, по своей сути вновь вводит определенную степень централизации, которая противоречит основополагающим принципам децентрализации. Прагматичный баланс между обеспечением юридической ответственности и сохранением основных преимуществ децентрализации, таких как отсутствие цензуры и содействие инновациям, требует постоянного обсуждения и потенциального развития гибридных правовых структур.

Наконец, хотя фактор вреда обеспечивает важную физическую связь, нематериальная и опосредованная цифровыми технологиями природа такого вреда, как психические страдания, ущерб репутации и ущерб, нанесенный цифровым двойникам, сопряжена с определенными сложностями в доказывании. Преодоление традиционного скептицизма в отношении виртуального характера вреда требует разработки новых методологий исследований, а также адаптации правил доказывания для учета и оценки этих новых форм цифровых доказательств.

Следовательно, будущие исследования должны сосредоточиться на ряде важных направлений. Во-первых, целесообразно провести сравнительные правовые исследования для выяснения того, как различные юрисдикции в настоящее время справляются с этими проблемами, и для выявления передовой практики трансграничного сотрудничества в расследованиях преступлений, связанных с метавселенной. Во-вторых, крайне важна разработка стандартизированных международных протоколов об обмене данными и взаимной правовой помощи в вопросах поиска и сбора доказательств, основанных на технологии блокчейн. В-третьих, междисциплинарные исследования с участием правоведов, специалистов в области информатики являются определяющими для уточнения технического и концептуального понимания цифровой личности, права собственности на цифровые активы и характера ущерба в виртуальных средах. Наконец, как представляется, законодательные инициативы должны выйти за рамки реактивной адаптации и проактивно создавать комплексные правовые рамки, которые по своей сути будут масштабируемыми и устойчивыми к быстрым технологическим изменениям, характерным для метавселенной. Только благодаря таким согласованным и совместным усилиям международное сообщество может надеяться на создание надежной и справедливой системы правосудия в зарождающейся цифровой среде метавселенной.

Список литературы

- Есаков, Г. А. (2015). Экстратерриториальное действие уголовного закона: современные мировые тенденции. *Закон*, 8, 82–89. <https://elibrary.ru/uhlbaf>
- Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, 19, 644–652. <https://doi.org/10.62441/nano-ntp.v19i3.5078>
- Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.
- Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, 32(1), 80–97. EDN: <https://elibrary.ru/fgebbr>. DOI: <https://doi.org/10.1108/JFRC-04-2023-0065>

- Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, 32(8), 605–646. EDN: <https://elibrary.ru/bxivih>. DOI: <https://doi.org/10.1002/jsid.2001>
- Brey, P. (2025). Will There Be a Metaverse? In *The Metaverse: A Critical Assessment*. SpringerBriefs in Ethics (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3
- Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, 35(1), 29–54. EDN: <https://elibrary.ru/gqkwgf>. DOI: <https://doi.org/10.1017/S0922156521000534>
- Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, 28(2), zmac031. EDN: <https://elibrary.ru/qlwgxi>. DOI: <https://doi.org/10.1093/jcmc/zmac031>
- Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, 232, 2310–2320. EDN: <https://elibrary.ru/skunaz>. DOI: <https://doi.org/10.1016/j.procs.2024.02.050>
- Ioannidis, S., & Kontis, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, 3(2), 152–165. EDN: <https://elibrary.ru/mwvqcn>. DOI: <https://doi.org/10.57019/jmv.1294970>
- Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, 44(1), 85–97. <https://doi.org/10.1093/polsoc/puae020>
- Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, 51(3), 142–152. <https://doi.org/10.1093/hcr/hqaf005>
- Komalavalli, C., Saxena, D., & Laroia, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press. <https://doi.org/10.1016/B978-0-12-819816-2.00014-9>
- McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, 36(1), 13. EDN: <https://elibrary.ru/rgzoum>. DOI: <https://doi.org/10.1007/s13347-023-00613-y>
- Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, 98, 917.
- Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, 4(1), 21–32. <https://doi.org/10.57019/jmv.1344489>
- Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). <https://doi.org/10.1002/9781394177165.ch4>
- Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, 23(2), 175–238. EDN: <https://elibrary.ru/ipnrgk>. DOI: <https://doi.org/10.1163/15718123-bja10151>
- Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. <https://doi.org/10.4018/979-8-3693-7630-0>
- Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. <https://doi.org/10.4324/9781003512677>
- Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 53(4), 2073–2082. <https://doi.org/10.1109/TSMC.2022.3228530>
- Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, 73, 102684. EDN: <https://elibrary.ru/sxufzu>. DOI: <https://doi.org/10.1016/j.ijinfomgt.2023.102684>
- Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, 10(2), 636. EDN: <https://elibrary.ru/hgwqbi>. DOI: <https://doi.org/10.3390/app10020636>
- Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24(3), 537–550. EDN: <https://elibrary.ru/dbquas>. DOI: <https://doi.org/10.1017/glj.2023.24>
- Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3
- Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, 10(2), 213–242. EDN: <https://elibrary.ru/kjghty>. DOI: <https://doi.org/10.1093/jfr/fjad014>

- Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, 22(14), 5396. EDN: <https://elibrary.ru/whsffs>. DOI: <https://doi.org/10.3390/s22145396>
- Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, 23(1), 146. EDN: <https://elibrary.ru/rxwauu>. DOI: <https://doi.org/10.3390/s23010146>
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1. EDN: <https://elibrary.ru/kwtfwh>. DOI: <https://doi.org/10.1186/s40163-021-00163-8>
- Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, 27(1), 49–67. <https://doi.org/10.1080/14606925.2023.2279836>
- Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

Сведения об авторе



Маджумаев Мурад Мамедович – кандидат юридических наук, ведущий научный сотрудник, старший преподаватель кафедры уголовного права, уголовного процесса и криминалистики Юридического института, Российский университет дружбы народов имени Патриса Лумумбы

Адрес: 117198, Россия, г. Москва, ул. Миклухо-Маклая, 6

E-mail: murad.mad@outlook.com

ORCID ID: <https://orcid.org/0000-0003-3332-2850>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58624042900>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/ABB-9737-2021>

Google Scholar ID: <https://scholar.google.com/citations?user=qpGC84MAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1212027

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование выполнено за счет гранта Российского научного фонда № 25-28-01478. <https://rscf.ru/project/25-28-01478/>

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс

Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 21 августа 2025 г.

Дата одобрения после рецензирования – 4 сентября 2025 г.

Дата принятия к опубликованию – 20 декабря 2025 г.

Дата онлайн-размещения – 25 декабря 2025 г.



Research article

UDC 34:004:343.213.3:343.232:343.235.4

EDN: <https://elibrary.ru/rowsaq>

DOI: <https://doi.org/10.21202/jdtl.2025.23>

Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse*

Murad M. Madzhumaev

Peoples' Friendship University of Russia named after Patrice Lumumba, Moscow, Russia

Keywords

augmented reality,
avatar,
crime,
crime scene,
criminal law,
digital technologies,
jurisdiction,
law,
metaverse,
virtual reality

Abstract

Objective: to critically analyze the possibility of extending the existing spatial criminal law principles to acts committed in the decentralized virtual worlds of the metaverse, and to develop proposals that include updating the approach to establishing jurisdiction over such virtual crimes.

Methods: the methodological basis of the research is a set of general scientific methods and approaches of scientific cognition – dialectical, formal logical (analysis and synthesis, induction and deduction), systematic, as well as private scientific methods – formal legal, legal modeling, interpretation. The study relies on an analysis of judicial practice, foreign legislation, technical features of blockchain technologies and decentralized autonomous organizations, which makes it possible to identify gaps in legal regulation and propose conceptually new solutions for determining the crime scene in a virtual environment.

Results: the study revealed a limited implementation of the current generally accepted principles of determining jurisdiction in relation to virtual crimes that do not have physical coordinates. The proposed multifactorial jurisdiction model redefines the “crime scene” taking into account factors such as the offender’s digital identity, the nature and location of digital assets, platform management protocols, and the actual damage caused. Assumingly, the immutable and verifiable nature of blockchain transactions can serve as a legal equivalent of a physical presence to establish personal jurisdiction, allowing criminal prosecution to be initiated even in cases where the actual location of the offender remains unknown.

© Madzhumaev M. M., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: the paper presents an approach that implies the fundamental transformation of reactive, adaptive legal regulation principles into a proactive, comprehensive framework designed specifically for the unique challenges of the metaverse. A paradigm-changing hypothesis was put forward: that a permanent (stable) digital footprint of the offender in virtual spaces can serve to exercise jurisdiction. The model systematically presents the idea of harm as the most important link between virtual offenses and their consequences in the real world.

Practical significance: it is currently impossible to apply legal norms and rules to relations in the metaverse, taking into account their specifics. The main provisions and conclusions of the study can be used to improve the mechanisms of legal regulation of the metaverse and to form international protocols on data exchange and mutual legal assistance for searching and collecting evidence based on blockchain technology. They may help to develop legislative initiatives aimed at creating integrated legal mechanisms that are scalable and resistant to rapid technological changes, characteristic for the digital environment.

For citation

Madzhumaev, M. M. (2025). Multifactor Model of Jurisdiction: Reviewing Locus Delicti in a Decentralized Metaverse. *Journal of Digital Technologies and Law*, 3(4), 570–597. <https://doi.org/10.21202/jdtl.2025.23>

References

- Aakula, A., Sandhu, K., Srinivasan Venkataramanan, V., Alluri, R. R., & Saini, V. (2023). Forging Unbreakable Identities: The Biometric-Blockchain Nexus. *Nanotechnology Perceptions*, 19, 644–652. <https://doi.org/10.62441/nano-ntp.v19i3.5078>
- Bains, P., Ismail, A., Melo, F., & Sugimoto, N. (2022). Regulating the crypto ecosystem: The case of unbacked crypto assets. *International Monetary Fund*.
- Benson, V., Turksen, U., & Adamyk, B. (2024). Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*, 32(1), 80–97. <https://doi.org/10.1108/JFRC-04-2023-0065>
- Bhowmik, A. K. (2024). Virtual and augmented reality: Human sensory-perceptual requirements and trends for immersive spatial computing experiences. *Journal of the Society for Information Display*, 32(8), 605–646. <https://doi.org/10.1002/jsid.2001>
- Brey, P. (2025). Will There Be a Metaverse? In *The Metaverse: A Critical Assessment*. SpringerBriefs in Ethics (pp. 33–57). Springer, Cham. https://doi.org/10.1007/978-3-031-93471-1_3
- Chimni, B. S. (2022). The international law of jurisdiction: A TWAIL perspective. *Leiden Journal of International Law*, 35(1), 29–54. <https://doi.org/10.1017/S0922156521000534>
- Esakov, G. A. (2015). Extraterritorial criminal jurisdiction: contemporary global trends. *Statute*, 8, 82–89. (In Russ.).
- Han, E., Miller, M. R., DeVeaux, C., Jun, H., Nowak, K. L., Hancock, J. T., Ram, N., & Bailenson, J. N. (2023). People, places, and time: a large-scale, longitudinal study of transformed avatars and environmental context in group interaction in the metaverse. *Journal of Computer-Mediated Communication*, 28(2), zmac031. <https://doi.org/10.1093/jcmc/zmac031>
- Hosseini, S., Abbasi, A., Magalhaes, L. G., Fonseca, J. C., da Costa, N. M., Moreira, A. H., & Borges, J. (2024). Immersive interaction in digital factory: Metaverse in manufacturing. *Procedia Computer Science*, 232, 2310–2320. <https://doi.org/10.1016/j.procs.2024.02.050>

- Ioannidis, S., & Kontis, A. P. (2023). The 4 Epochs of the Metaverse. *Journal of Metaverse*, 3(2), 152–165. <https://doi.org/10.57019/jmv.1294970>
- Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: rethinking regulation for artificial intelligence. *Policy and Society*, 44(1), 85–97. <https://doi.org/10.1093/polsoc/puae020>
- Kim, H. S., Kim, S., & Lee, E. J. (2025). The mirror of the metaverse: an exploration of reciprocal effects between self-views and avatar-based self-presentation. *Human Communication Research*, 51(3), 142–152. <https://doi.org/10.1093/hcr/hqaf005>
- Komalavalli, C., Saxena, D., & Laroia, C. (2020). Overview of blockchain technology concepts. In *Handbook of research on blockchain technology* (pp. 349–371). Academic Press.
- McStay, A. (2023). The metaverse: Surveillant physics, virtual realist governance, and the missing commons. *Philosophy & Technology*, 36(1), 13. <https://doi.org/10.1007/s13347-023-00613-y>
- Niesel, Z. (2023). Crypto Contacts: Jurisdiction and the Blockchain. *Tulane Law Review*, 98, 917.
- Özkan, A., & Özkan, H. (2024). Meta: XR-AR-MR and mirror world technologies business impact of metaverse. *Journal of Metaverse*, 4(1), 21–32. <https://doi.org/10.57019/jmv.1344489>
- Panda, S. K. (2023). Revolution of the metaverse and blockchain technology. In *Metaverse and immersive technologies: An introduction to industrial, business and social applications* (pp. 97–125). <https://doi.org/10.1002/9781394177165.ch4>
- Payer, A. (2023). The Territorial Principle as a Basis for State Criminal Jurisdiction: Particularly with Regard to Cross-Border Offences and Attempts, and to Multiple Parties to an Offence Acting in Different Countries. *International Criminal Law Review*, 23(2), 175–238. <https://doi.org/10.1163/15718123-bja10151>
- Pesqueira, A. (2025). The Impact and Potential. In A. Pesqueira, & A. de Bem Machado (Eds.), *Navigating Privacy, Innovation, and Patient Empowerment Through Ethical Healthcare Technology* (pp. 217–254). IGI Global. <https://doi.org/10.4018/979-8-3693-7630-0>
- Pogorzelska, K. (2024). Does Using Satellite Data for Sustainable Development Justify Unsustainable Use of Outer Space? In *Regulation of Outer Space* (pp. 7–25). Routledge. <https://doi.org/10.4324/9781003512677>
- Qin, R., Ding, W., Li, J., Guan, S., Wang, G., Ren, Y., & Qu, Z. (2022). Web3-based decentralized autonomous organizations and operations: Architectures, models, and mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 53(4), 2073–2082. <https://doi.org/10.1109/TSMC.2022.3228530>
- Richter, S., & Richter, A. (2023). What is novel about the Metaverse? *International Journal of Information Management*, 73, 102684. <https://doi.org/10.1016/j.ijinfomgt.2023.102684>
- Rokhsaritalemi, S., Sadeghi-Niaraki, A., & Choi, S. M. (2020). A review on mixed reality: Current trends, challenges and prospects. *Applied Sciences*, 10(2), 636. <https://doi.org/10.3390/app10020636>
- Ryngaert, C. (2023). Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts. *German Law Journal*, 24(3), 537–550. <https://doi.org/10.1017/glj.2023.24>
- Scharfman, J. (2024). Decentralized autonomous organization (dao) fraud, hacks, and controversies. In *The Cryptocurrency and Digital Asset Fraud Casebook, Volume II: DeFi, NFTs, DAOs, Meme Coins, and Other Digital Asset Hacks* (pp. 65–106). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-60836-0_3
- Schuler, K., Cloots, A. S., & Schär, F. (2024). On DeFi and on-chain CeFi: how (not) to regulate decentralized finance. *Journal of Financial Regulation*, 10(2), 213–242. <https://doi.org/10.1093/jfr/fjad014>
- Segovia, M., & Garcia-Alfaro, J. (2022). Design, modeling and implementation of digital twins. *Sensors*, 22(14), 5396. <https://doi.org/10.3390/s22145396>
- Syed, T. A., Siddiqui, M. S., Abdullah, H. B., Jan, S., Namoun, A., Alzahrani, A., Nadeem, A., & Alkhodre, A. B. (2022). In-depth review of augmented reality: Tracking technologies, development tools, AR displays, collaborative AR, and security concerns. *Sensors*, 23(1), 146. <https://doi.org/10.3390/s23010146>
- Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, 11(1), 1. <https://doi.org/10.1186/s40163-021-00163-8>
- Wei, W. (2023). Using actor–network theory to revisit the digitalized tool in social design. *The Design Journal*, 27(1), 49–67. <https://doi.org/10.1080/14606925.2023.2279836>
- Wendehorst, C. (2023). Proprietary rights in digital assets and the conflict of laws. In *Blockchain and Private International Law* (pp. 101–127). Brill Nijhoff. https://doi.org/10.1163/9789004514850_007

Author information



Murad M. Madzhumaev – Cand. Sci. (Law), Leading researcher, Senior Lecturer, Department of Criminal Law, Criminal Procedure and Criminology, Institute of Law, Peoples' Friendship University of Russia named after Patrice Lumumba

Address: 6 Miklukho-Maklaya Str., 117198 Moscow, Russia

E-mail: murad.mad@outlook.com

ORCID ID: <https://orcid.org/0000-0003-3332-2850>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=58624042900>

WoS Researcher ID: <https://www.webofscience.com/wos/author/record/ABB-9737-2021>

Google Scholar ID: <https://scholar.google.com/citations?user=qpGC84MAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1212027

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research was made under the grant of the Russian Scientific Fund No. 25-28-01478. <https://rscf.ru/project/25-28-01478/>

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – August 21, 2025

Date of approval – September 4, 2025

Date of acceptance – December 20, 2025

Date of online placement – December 25, 2025