УДК 341.1

Кэфэй Ся
(магистрант Белорусского государственного университета)

ПОНЯТИЕ, ОСОБЕННОСТИ И ПРАВОВАЯ ПРИРОДА КИБЕРПРОСТРАНСТВА

В статье представлено научное исследование концептуальных основ и правовой сущности киберпространства как новой социально-технической реальности. Статья посвящена решению комплексной проблемы, связанной с несоответствием традиционных правовых парадигм и категорий уникальным свойствам киберпространства. Ключевые аспекты проблематики включают: преодоление юрисдикционных коллизий, вызванных трансграничным характером данной среды; правовую квалификацию виртуальных деяний, влекущих материальные последствия; поиск баланса между регулированием, саморегулированием и анонимностью; а также адаптацию классических правовых институтов к таким новым явлениям, как криптоактивы, смарт-контракты и метавселенные. Новизна исследования заключается в обосновании гибридной и плюралистической правовой природы киберпространства. В работе доказывается, что его регулирование представляет собой не иерархическую систему, а динамичное взаимодействие («переплетение») национального законодательства, норм международного права и транснационального частного регулирования, где формальный закон уравнивается с таким мощным регулятором, как программный код («code is law»). Такой интегративный подход позволяет выработать более адекватные и эффективные правовые стратегии для управления цифровой средой.

Киберпространство как феномен современности представляет собой сложный и многогранный объект научного осмысления, оказывающий трансформационное воздействие на все сферы человеческой жизнедеятельности, включая право [1]. Его возникновение и развитие обусловлены цифровой революцией, которая не просто создала новые инструменты коммуникации, но и сформировала принципиально иную среду существования социальных отношений. Понимание понятия, сущностных особенностей и правовой природы киберпространства является фундаментальной задачей для юриспруденции, поскольку именно право призвано упорядочивать возникающие в этой новой реальности общественные связи, обеспечивать в ней баланс интересов, безопасность и защиту прав.

Изначально термин «киберпространство», введенный в научный оборот Уильямом Гибсоном, носил скорее метафорический характер, описывая коллективную галлюцинацию, консенсуальную иллюзию. Однако с развитием глобальных сетей, прежде всего Интернета, это понятие наполнилось реальным содержанием. В современной доктрине киберпространство принято определять как глобальную динамическую область, образуемую совокупностью информационных систем и сетей телекоммуникаций, взаимодействующих на основе единых стандартов и протоколов, в которой посредством цифровых технологий создается, хранится, обрабатывается и передается информация, и где осуществляются социальные, экономические, политические и иные взаимодействия между людьми, организациями и автоматизированными системами. Это не просто техническая инфраструктура, а именно социально-техническая система, виртуальная среда, в которой протекают значимые для общества процессы [2].

Ключевой особенностью киберпространства, определяющей все его остальные свойства, является его трансграничность. Физические границы

государств, являющиеся краеугольным камнем традиционного международного и национального права, в киберпространстве теряют свое определяющее значение. Информационный поток, цифровая транзакция или кибератака могут быть инициированы с территории одного государства, направлены через серверы, расположенные в нескольких других странах, и оказать воздействие на пользователей или критическую инфраструктуру в третьих государствах. Эта атрибутивная черта ставит под сомнение классическую юрисдикционную модель, основанную на территориальности, и порождает сложнейшие коллизии правоприменения. С трансграничностью неразрывно связана виртуальность киберпространства. Процессы и объекты в нем не имеют материального воплощения в традиционном понимании, существуя в виде данных, битов и байтов. Однако эта виртуальность порождает совершенно реальные правовые последствия: заключаются договоры, передаются права собственности на цифровые активы (например, токены или NFT), причиняется вред, совершаются преступления [3].

Таким образом, киберпространство представляет собой парадоксальную среду, где виртуальное действие влечет материальные юридически значимые результаты. Еще одной фундаментальной особенностью является его децентрализованность и анонимность (или псевдоанонимность). В отличие от иерархически организованных структур традиционного общества, киберпространство по своей архитектуре является сетевым и распределенным. Отсутствие единого контролирующего центра затрудняет регулирование и привлечение к ответственности. Анонимность, обеспечиваемая техническими средствами, с одной стороны, выступает гарантом приватности и свободы выражения, а с другой – создает благоприятную почву для киберпреступности, распространения запрещенного контента и иных злоупотреблений.

Правовая природа киберпространства является предметом острой научной дискуссии. Можно выделить несколько основных подходов к ее пониманию. Согласно первой, наиболее консервативной позиции, киберпространство не является особым правовым объектом. Оно представляет собой лишь новую технологическую среду, в которой действуют уже существующие правовые нормы. С этой точки зрения, нет необходимости создавать специальное «киберправо», а достаточно адаптировать и применять традиционные институты гражданского, уголовного, административного права к новым реалиям [4].

Например, сделка, заключенная онлайн, квалифицируется как договор в письменной форме, а несанкционированный доступ к компьютерной информации – как преступление против собственности или общественной безопасности. Однако данный подход сталкивается с серьезными ограничениями, так как многие феномены киберпространства, такие как криптовалюты, смарт-контракты, метавселенные, виртуальная личность, не укладываются в прокрустово ложе классических юридических конструкций. Второй, радикальный подход, сформировавшийся на заре интернета, напротив, провозглашал киберпространство особым суверенным пространством, полностью свободным от государственного регулирования [5]. Сторонники этой точки зрения, такие как Джон Перри Барлоу в своей «Декларации независимости

киберпространства», утверждали, что традиционные правительства не обладают легитимностью для установления правил в этой новой «цифровой цивилизации», которая должна выработать собственные, основанные на саморегулировании и сетевых нормах, механизмы упорядочивания. Хотя эта утопическая идея в чистом виде не реализовалась, ее отголоски живут в принципах децентрализованных систем (блокчейн) и в идеологии технолибертарианства [6].

Наиболее адекватной представляется третья, комплексная позиция, согласно которой киберпространство представляет собой гибридную правовую среду. Это особая сфера, где переплетаются и взаимодействуют несколько регуляторных систем: национальное законодательство отдельных государств, пытающееся экстраполировать свою юрисдикцию на трансграничные процессы; международное право, формирующееся через резолюции ООН, конвенции Совета Европы и иные многосторонние соглашения; и, наконец, транснациональное частное регулирование, включающее в себя технические стандарты (протоколы TCP/IP, DNS), правила платформ (политика Facebook, Google, Apple), отраслевые кодексы поведения и, что особенно важно, код как закон. Тезис Лоуренса Лессига о том, что «архитектура есть политика», в полной мере применим к киберпространству: программный код, определяющий его устройство и функционирование, де-факто является мощнейшим регулятором, зачастую более эффективным, чем правовые нормы.

Таким образом, правовая природа киберпространства плюралистична: оно регулируется не только государственным законом, но и сложным конгломератом формальных и неформальных правил, создаваемых как государственными, так и негосударственными акторами. Это ставит перед правом вызовы беспрецедентного масштаба. Во-первых, это вызов юрисдикции. Какому государству подчиняется сайт, размещенный на сервере в одной стране, администрируемый гражданином другой и посещаемый пользователями со всего мира? Принципы «страны назначения», «страны происхождения» или «наличия целевой аудитории» порождают противоречия. Во-вторых, это вызов правоприменению. Высокая скорость изменений, анонимность и трансграничность делают традиционные механизмы раскрытия преступлений, получения доказательств и исполнения решений крайне затруднительными. Требуются новые формы международного сотрудничества, такие как заключение соглашений о прямом доступе правоохранительных органов к данным в экстренных ситуациях. В-третьих, это вызов защите фундаментальных прав. В киберпространстве с новой силой встают вопросы о соотношении свободы слова и контроля за контентом, о праве на приватность и обязанности государств обеспечивать безопасность, о защите персональных данных в условиях их тотальной коммерциализации и использования искусственным интеллектом.

Современный этап развития правового регулирования киберпространства характеризуется переходом от фрагментированных и реактивных мер к построению целостных проактивных систем. Это находит отражение в принятии комплексных национальных стратегий кибербезопасности, развитии законодательства о защите критической информационной инфраструктуры,

установлении жестких требований к обработке персональных данных (как, например, в Регламенте GDPR в ЕС и его аналогах в других странах) [7].

Активно развивается и международное киберправо, о чем свидетельствует работа специализированных групп экспертов ООН по вопросам ответственности государств в киберпространстве и применения к нему норм международного гуманитарного права. Правовая природа киберпространства продолжает эволюционировать с появлением новых технологий. Блокчейн и смарт-контракты бросают вызов традиционному договорному праву и представлениям о доверии. Искусственный интеллект, способный к автономному принятию решений, ставит вопросы о деликтоспособности и правосубъектности. Метавселенные, создающие immersive-среды для работы, учебы и отдыха, порождают споры о праве собственности на виртуальные объекты и землю, о юрисдикции внутри этих цифровых миров. В заключение следует отметить, что киберпространство не является статичным объектом. Это динамичная, постоянно усложняющаяся среда, которая продолжает бросать вызов традиционным правовым парадигмам. Его понятие охватывает не только технологическую инфраструктуру, но и всю совокупность социальных отношений, опосредованных цифровыми технологиями. Его особенности – трансграничность, виртуальность, децентрализация – являются источником как новых возможностей, так и новых угроз.

Таким образом, правовая природа киберпространства носит гибридный и плюралистический характер, представляя собой сложное переплетение национального, международного и транснационального регулирования, где закон конкурирует и взаимодействует с кодом и сетевыми нормами. Дальнейшее развитие права в этой сфере будет зависеть от способности правовых систем к гибкости, адаптации и международной кооперации для обеспечения в киберпространстве верховенства права, защиты прав человека и устойчивого развития цифрового общества.

Список использованной литературы

1. Абрамов, Р. А. Правовая природа киберпространства и вызовы современному праву / Р. А. Абрамов // Lex russica. – 2022. – Т. 75, № 12. – С. 9–22.

2. Войниканис, Е. А. Право и цифровизация: новые вызовы и перспективы / Е. А. Войниканис // Журнал зарубежного законодательства и сравнительного правоведения. – 2021. – Т. 17, № 4. – С. 5–19.

3. Кашкин, С. Ю. Международно-правовое регулирование киберпространства: современные тенденции и противоречия / С. Ю. Кашкин, А. О. Четвериков // Московский журнал международного права. – 2023. – № 1. – С. 6–25.

4. Полякова, Т. А. Правовое обеспечение цифровой безопасности: теоретические и практические аспекты / Т. А. Полякова. – М. : Юстицинформ, 2022. – 188 с.

5. Селивановский, А. С. Гражданское право в условиях цифровой трансформации / А. С. Селивановский. – М. : Статут, 2021. – 256 с.

6. Талимончик, В. П. Трансграничное потоков данных и национальная юрисдикция: проблемы и модели регулирования / В. П. Талимончик // Международное правосудие. – 2023. – № 1. – С. 45–58.

7. Чучаев, А. И. Уголовно-правовые и криминологические аспекты киберпреступности / А. И. Чучаев, А. Г. Хабибулин. – М. : Проспект, 2022. – 192 с.