УДК 347.5

ЦИВИЛИСТИЧЕСКИЕ АСПЕКТЫ РАСПРЕДЕЛЕНИЯ РИСКОВ ПРИ ЭКСПЛУАТАЦИИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Бельдина О.Г.

старший преподаватель,

Уральский государственный экономический университет,

Екатеринбург, Россия

Аннотация

В статье исследуются концептуальные подходы к определению гражданско-правовой ответственности за вред, причиненный автономными системами искусственного интеллекта (ИИ). Рассматриваются модели распределения рисков: аналогия с источником повышенной опасности, а также договорные механизмы распределения ответственности. Показывается взаимосвязь между уровнем цифровой зрелости отраслей экономики и готовностью правовой системы к восприятию новых технологических рисков. Делается вывод о целесообразности комбинированного применения внедоговорных и договорных конструкций для сбалансированного стимулирования инноваций и защиты прав третьих лиц.

Ключевые слова: искусственный интеллект, гражданско-правовая ответственность, источник повышенной опасности, деликт, договорные риски, презумпция причинения вреда, секрет производства, конфиденциальная информация.

CIVILISTIC ASPECTS OF RISK ALLOCATION IN THE OPERATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

Beldina O.G.

Senior Lecturer,

Ural State University of Economics,

Ekaterinburg, Russia

Abstract

The article examines conceptual approaches to determining civil liability for harm caused by autonomous artificial intelligence (AI) systems. The author analyzes models of risk distribution, including the analogy with a source of increased danger, as well as contractual mechanisms for allocating liability. The interrelation between the level of digital maturity in various economic sectors and the legal system's readiness to address emerging technological risks is demonstrated. It is concluded that a combined application of non-contractual and contractual legal constructs is advisable for achieving a balanced stimulation of innovation while protecting the rights of third parties.

Keywords: artificial intelligence, civil liability, source of increased danger, tort, contractual risks, presumption of causation, trade secret, confidential information.

Внедрение систем искусственного интеллекта в критически важные инфраструктуры (беспилотный транспорт, медицинская диагностика, кредитный скоринг, государственное управление) актуализирует проблему пересмотра оснований и условий гражданско-правовой ответственности. Классические институты деликтного и договорного права, ориентированные на волевое поведение дееспособного субъекта, оказываются в ситуации когнитивного диссонанса, когда решение, повлекшее вред, сгенерировано автономным алгоритмом, чья логика не была непосредственно запрограммирована человеком.

Стремительный рост вычислительных мощностей, доступность больших данных и совершенствование методов глубокого обучения привели к тому, что современные ИИ-системы демонстрируют поведение, которое разработчики зачастую не могут предсказать или ретроспективно объяснить. Традиционные условия наступления ответственности (противоправность, вред, причинная

связь, вина) требуют существенной адаптации, особенно в части установления субъекта.

По мере возрастания автономии ИИ-систем и способности машин к самообучению человеческий контроль над их поведением становится все более ограниченным, а следовательно, классическая предпосылка ответственности - наличие субъекта, способного предвидеть и контролировать последствия своих действий, перестает работать. Если ни один человек не мог предвидеть конкретный вектор поведения машины, то привлечение к ответственности разработчика, владельца или пользователя оказывается юридически и этически спорным.

В российской цивилистической науке комплексный анализ проблемы ответственности за вред, причиненный ИИ, пока не получил завершенного оформления, однако отдельные аспекты исследуются в контексте правосубъектности электронных лиц, деликтной ответственности за автономные действия и договорных рисков при поставке программного обеспечения.

Жизненный цикл современной ИИ-системы включает последовательные, но юридически самостоятельные этапы: формирование дата-сетов, разработка архитектуры модели, обучение и валидация, интеграция в аппаратно-программный комплекс, эксплуатация, мониторинг и дообучение. Каждый из этих этапов контролируется разными субъектами - поставщиками данных, разработчиками ПО, производителями оборудования, системными интеграторами, операторами и конечными пользователями.

Возникает проблема «распределенного вреда», когда дефект, допущенный на раннем этапе (например, нерепрезентативность обучающей выборки), проявляется лишь на этапе эксплуатации, приводя к ущербу у третьих лиц. Установить конкретного виновного при таких обстоятельствах крайне сложно, особенно если договорные отношения между участниками не содержат четкого распределения рисков и технических спецификаций [8].

В российской судебной практике, хотя и немногочисленной по данной тематике, уже наблюдаются попытки квалификации недостатков сложного программного обеспечения по аналогии с правилами о поставке некачественного товара (ст. 475, 518 ГК РФ). Однако такой подход вызывает критику, поскольку цифровой продукт не обладает свойствами вещи, а его качество зависит от множества динамических факторов, включая корректность вводных данных и условия эксплуатации.

Одним из наиболее аргументированных подходов в доктрине является распространение на ИИ-системы режима ответственности владельца источника повышенной опасности (ст. 1079 ГК РФ). Эта аналогия обосновывается следующими соображениями:

- ИИ-системы, интегрированные в транспорт, промышленное оборудование или медицинские устройства, объективно создают повышенную вероятность причинения вреда жизни, здоровью или имуществу;

- ответственность владельца источника повышенной опасности наступает независимо от вины, что позволяет сместить фокус судебного разбирательства с субъективного психического отношения нарушителя на объективные обстоятельства причинения вреда [6];

- владелец, возместивший ущерб, не лишается права регресса к производителю или разработчику, если удастся доказать конструктивный дефект или нарушение требований стандартизации.

Вместе с тем, применение этой аналогии сталкивается с контраргументами. Во-первых, в отличие от источника повышенной опасности в классическом понимании (автомобиль, реактор), ИИ-система постоянно эволюционирует, и ее «опасность» зависит от качества данных и параметров дообучения, которые могут меняться в процессе эксплуатации. Во-вторых, режим источника повышенной опасности плохо приспособлен для компенсации нематериальных ущербов - дискриминации, репутационных потерь, нарушения

приватности, которые нередко являются следствием алгоритмических ошибок [7].

Тем не менее, пока специальное законодательство отсутствует, применение аналогии закона (ст. 6 ГК РФ) остается наиболее прагматичным инструментом для судов, позволяющим обеспечить защиту прав потерпевших и стимулировать владельцев ИИ-систем к страхованию рисков и внедрению систем мониторинга [10].

Отдельного внимания заслуживают договорные конструкции, опосредующие передачу ИИ-систем. В зависимости от формы поставки - программное обеспечение как самостоятельный объект, встроенный компонент оборудования (embedded) или облачный сервис (SaaS) - существенно различаются применимые нормы об ответственности.

Если система ИИ поставляется как неотъемлемая часть оборудования, ее недостатки могут квалифицироваться как дефект товара, что открывает возможность применения правил о купле-продаже и ответственности за недостатки качества (ст. 469–476 ГК РФ). В российской судебной практике встречаются решения, где недостижение ожидаемых функциональных характеристик программного комплекса трактуется как существенное нарушение договора, позволяющее требовать соразмерного уменьшения цены или расторжения договора [8].

Однако при передаче программного обеспечения по лицензионному договору предметом является не «качество» как полезное свойство, а право использования объекта интеллектуальной собственности. В этом случае гарантии качества могут быть установлены только специальными условиями договора, и их нарушение влечет ответственность по правилам ст. 450–453 ГК РФ о неисполнении обязательств, а не по правилам о товарных недостатках [12].

Поскольку системы ИИ функционируют на основе обработки значительных массивов информации, важное значение приобретает правовой режим самой информации, используемой для обучения и эксплуатации

алгоритмов. Как отмечает Н.А. Свалова, «главной целью у любой экономической, в том числе предпринимательской, деятельности человека является получение прибыли. Для этого он использует свои знания, умения и навыки для преодоления каких-либо негативных экономических факторов. В результате у субъектов предпринимательства накапливается свод информации, которая имеет коммерческую и иную ценность» [11]. Эта информация позволяет субъектам конкурировать на рынке, что особенно актуально для разработчиков ИИ-систем, чьи дата-сеты и алгоритмы представляют собой ключевые конкурентные активы.

В связи с этим встают вопросы о правовой защите такой информации: во-первых, о возможности защитить эту информацию от использования другими лицами; во-вторых, получить доход за счет передачи права на использование этой информации другим лицам [11]. В соответствии со ст. 6 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года обладатель информации может по своему усмотрению использовать «свою» информацию, разрешать или ограничивать доступ к ней, передавать ее другим лицам по договору [11].

Для секрета производства (ноу-хау) закон устанавливает специальный режим охраны в соответствии с гл. 75 ГК РФ. Для иной конфиденциальной информации обладатель может самостоятельно выбрать режим использования третьими лицами, назвав ее, например, «конфиденциальной», «корпоративной» и т.п., регламентируя все условия локальными актами и договорами [11]. Правовой режим секрета производства требует наличия совокупности признаков: действительная или потенциальная коммерческая ценность вследствие неизвестности третьим лицам; отсутствие свободного доступа к таким сведениям на законном основании; принятие обладателем разумных мер для соблюдения их конфиденциальности [11].

Этот аспект непосредственно связан с проблемами ответственности при разработке и применении ИИ: если в процессе эксплуатации системы происходит утечка или неправомерное использование конфиденциальных данных,

составляющих коммерческую тайну разработчика, возникает вопрос о гражданско-правовой ответственности как самого разработчика, так и оператора, допустившего нарушение режима защиты информации. Поэтому правовое регулирование оборота информации и защиты интеллектуальных прав является неотъемлемой частью общей системы управления рисками в сфере ИИ.

Эффективность любого правового механизма ответственности напрямую зависит от уровня технологического развития и организационной культуры в соответствующих отраслях.

Как справедливо отмечает О.А. Колодкина, «цифровая зрелость российской системы образования может рассматриваться в качестве определенного итога (результата) таких двух взаимосвязанных между собой процессов - цифровизация образования и цифровая трансформация образования» [9]. Этот тезис важен и для юридической науки, поскольку он указывает на то, что внедрение сложных цифровых продуктов в социальную практику должно сопровождаться синхронным развитием нормативной базы, стандартов и механизмов правовой защиты [2; 3]. Цифровая зрелость отрасли предполагает не только техническое оснащение, но и наличие у всех участников (разработчиков, операторов, контролирующих органов) компетенций по управлению рисками, включая риски гражданско-правовой ответственности.

Таким образом, переход от «цифровизации» (количественные изменения - внедрение интернета, электронного документооборота) к «цифровой трансформации» (качественные изменения бизнес-моделей и институциональных практик) требует пересмотра многих правовых институтов, включая институт возмещения вреда [1; 5; 10], вопросы защиты конфиденциальной информации и коммерческой тайны [11], а также правовой охраны результатов интеллектуальной деятельности [10; 12].

Проведенный анализ позволяет сформулировать ряд выводов, имеющих как доктринальное, так и практическое значение:

- единая модель ответственности для всех видов ИИ-систем невозможна ввиду разнообразия их архитектур, областей применения и уровней автономности. Необходим дифференцированный подход, учитывающий степень риска (высокий, средний, низкий) и характер причиненного вреда (физический, имущественный, нематериальный);

- сочетание внедоговорных и договорных конструкций при причинении вреда третьим лицам, наиболее адекватным остается подход к ИИ-системе как к источнику повышенной опасности с возможностью регрессных исков к производителям и разработчикам. Для внутренних отношений в цепочке поставки приоритетны договорные механизмы - четкое техническое задание, SLA-метрики, условия страхования и разграничения ответственности;

- введение обязательных стандартов качества данных, алгоритмической прозрачности и логирования, а также законодательно закрепленных опровержимых презумпций причинения вреда при нарушении этих стандартов позволит снизить бремя доказывания для потерпевших и создаст стимулы для добросовестного поведения разработчиков [6];

- поскольку ИИ-системы оперируют массивами данных, имеющих коммерческую ценность, необходимо обеспечить адекватный правовой режим защиты конфиденциальной информации и секретов производства (ноу-хау), включая договорные механизмы неразглашения и ответственность за их нарушение [11; 12].

- уровень правовой защищенности в цифровой сфере неразрывно связан с общим уровнем цифровой зрелости общества и отраслей экономики, поэтому развитие правовых институтов должно идти рука об руку с технологической модернизацией и повышением квалификации участников оборота [9; 4].

Перспективными направлениями дальнейших исследований являются: разработка типовых договорных моделей для передачи ИИ-систем с учетом правового режима информации и ноу-хау, анализ страховых механизмов как

инструмента распределения рисков, а также сравнительно-правовые исследования подходов к ответственности в различных странах.

Библиографический список:

1. Алиева Э.Ф., Резапкина Г.В., Алексеева А.С., Ванданова Э.Л., Карташова Е.В. Цифровая переподготовка. Обучение родителей образовательных организаций // Образовательная политика. 2020. - № 1 (81). С. 52–59.

2. Бурлака С.Н. Цифровизация образования: проблемы развития // Тенденции развития электронного образования в России и за рубежом: мат-лы I Междунар. науч.-практ. конф. (Екатеринбург, 15 мая 2020 г.). Екатеринбург: УрГЭУ, 2020. - 221 с.

3. Екимова Н.В. Цифровизация в образовании: происхождение термина и психологические особенности сути феномена // Психология. Историко-критические обзоры и современные исследования. 2021. Т. 10, № 4А. - С. 165–171.

4. Качкова О.Е., Егупова О.А. Образование как отрасль социальной сферы // Социальная политика и социология. 2009. № 7. - С. 348–355.

5. Колоткина О.А. Основные направления цифровизации образовательного процесса в условиях развития высшего образования // Цифровая экономика и онлайн-образование: ключевые тренды и препятствия: мат-лы IV Междунар. науч.-практ. конф. (Екатеринбург, 28 мая 2024 г.). Екатеринбург: УрГЭУ, 2024. - С. 236–238.

6. Морозова Г.М. Современные технологии дистанционного обучения, применяемые в сфере среднего профессионального образования // Современный учитель – взгляд в будущее: сб. науч. ст. междунар. науч.-образов. форума (Екатеринбург, 17–18 ноября 2022 г.). Екатеринбург, 2022. - С. 45–48.

7. Трудности и перспективы цифровой трансформации образования / А.Ю. Уваров, Э. Гейбл, И.В. Дворецкая и др.; под ред. А.Ю. Уварова, И.Д. Фрумина. М.: Высшая школа экономики, 2019. - 344 с.

8. Цифровая трансформация: ожидания и реальность: докл. к XXIII Ясинской (Апрельской) междунар. науч. конф. по проблемам развития экономики и общества (Москва, 2022 г.) / Г.И. Абдрахманова, С.А. Васильковский, К.О. Вишневский и др. М.: Высшая школа экономики, 2022. - 221 с.

9. Колоткина О.А. Цифровая зрелость образования как национальная цель развития Российской Федерации / О.А. Колоткина // Цифровая экономика и онлайн-образование: ключевые тренды и препятствия: материалы V Междунар. науч.-практ. конф. - Екатеринбург: УрГЭУ, 2025. - С. 167–169.

10. Морхат П.М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис. … д-ра юрид. наук. М., 2018. 420 с.

11. Свалова Н.А. Правовой режим информации ограниченного использования в предпринимательской деятельности / Н.А. Свалова // Экономико-правовые проблемы обеспечения экономической безопасности: материалы VIII Международной научно-практической конференции. - Екатеринбург, 2025. - С. 88–91.

12. Цепов Г.В., Иванов Н.В. К цивилистической теории смарт-контрактов // Закон. 2022. № 3. - С. 149–172.