ПРИЗНАНИЕ ОШИБКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ОБСТОЯТЕЛЬСТВОМ НЕПРЕОДОЛИМОЙ СИЛЫ КАК ФАКТОР ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ЦИФРОВОГО СУВЕРЕНИТЕТА ГОСУДАРСТВА

В.А. Новицкий
В.В. Паршонков
Санкт-Петербургский университет технологий управления и экономики

Аннотация

С развитием технологий дефиниция цифрового суверенитета вызывает все больший интерес в юридической литературе. Технологическое развитие трансформирует взаимоотношения между людьми, преобразует государственную роль в правовом регулировании таких отношении, а также обуславливает необходимость углубления и расширения исследования таких базовых правовых институтов. Авторы отмечают, что при исследовании данной проблемы особое место следует уделить таким категориям как «воля» и «ответственность», т.к. именно данные категории играют особую роль в обеспечении государственного контроля в цифровой сфере.

Ключевые слова: искусственный интеллект, обстоятельство непреодолимой силы, форс-мажор, ответственность, ошибки искусственного интеллекта, цифровизация, защита суверенитета.

В последнее время особое внимание привлекает прогресс в сфере роботизации и автоматизации с использованием искусственного интеллекта (далее – ИИ). Развитие в данной сфере вызывает немало вопросов, связанных с урегулированием правоотношений, которые возникают в связи с использованием ИИ, в т.ч. об обеспечении цифрового суверенитета государства, т.к. обеспечение безопасности государства предполагает защиту прав и свобод граждан в цифровом пространстве, что вытекает из Конституции Российской Федерации.

Любое государство в настоящее время заинтересовано в увеличении темпов цифровизации. Вместе с тем нельзя не учитывать, что вместе с экономическим развитием цифровизации затрагивает и вопрос обеспечения цифрового суверенитета государства. Так некоторые авторы уже высказали идею о том, что использование ИИ может вовсе лишить государство его суверенитета в том случае, если на ИИ будут возложены ключевые алгоритмы управления государством [1].

Очевидно, что широкое распространение ИИ в таких сферах как здравоохранение, образование, военная промышленность напрямую затрагивает вопрос экономической безопасности и суверенитета страны.

Следует отметить, что на данный момент не сформировалось устоявшееся понимание понятия «цифровой суверенитет» [2], что обусловлено отсутствием критериальных признаков [3].

Как верно отмечает Петроченков И.А., «текущее нормативное правовое регулирование информационных технологий и информационного пространства носит фрагментарный и ситуативный характер, в том числе в связи с отсутствием базового понятия цифрового суверенитета. Механизмы правового обеспечения суверенитета Российской Федерации не реализованы системно в отношении информационной сферы» [3].

Узкое толкование предполагает, что цифровой суверенитет не отличается от информационного и сводится к праву государства контролировать информацию на его территории [4].

В широком смысле цифровой суверенитет обусловлен на использование отечественного IT-оборудования и приоритетную поддержку отечественных IT-компаний в цифровой сфере, а также обеспечение гарантий безопасности во внутренней интернет-инфраструктуре государства, и при использовании иных цифровых технологий [5].

В настоящий момент юридическая наука, и тем более законодатель, не успевают за высокими темпами цифровизации, вследствие чего в правоотношениях возникают «серые зоны» в нормативном регулировании. Очевидно, что обеспечение суверенитета невозможно без нормативного регулирования отношений, поскольку оно задает вектор правоотношений, а также позволяет делать их предсказуемыми.

Доктрина информационной безопасности в Российской Федерации выделяет особое место защите цифрового суверенитета Российской Федерации [6]. Так, Национальная стратегия развития ИИ до 2030 года закрепляет, что использование технологий ИИ отнесено к одному из целей для достижения цифрового суверенитета [7]. В настоящее время значимость обеспечения цифрового суверенитета возрастает из-за ускорения процессов цифровой интеграции международных организаций стран Евразийского экономического союза (далее – ЕАЭС), в т.ч. для целей сохранение национальной безопасности государств-членов, что отражено в решении Высшего Евразийского экономического совета [8].

Как верно отмечают Баранова А.Ф. и Шмагун Е.С., построение собственной цифровой экосистемы даже на территории одного государства требует серьезных правовых нововведений и преобразований [9]. Однако именно посредством нормативного регулирования государство сможет обеспечить устойчивое развитие в цифровой сфере.

Вместе с тем в сложившихся условиях следует уделять внимание не только разработке нового регулирования оборота в цифровой сфере, но исследовать вопрос о возможности применения уже существующих институтов к цифровым инновациям, таким как ИИ, расширенная (дополненная) реальность, робототехника, блокчейн технологии и т.д.

В научной литературе прослеживается тенденция на наращивание понятийного аппарата, выделение новых аспектов общественных отношений

[10], трансформация нормативного регулирования цифровой среды в сторону интенсификации [11]

Одновременно с тем «14» июня 2023 года Европейский парламент принял свою позицию на переговорах по Закону об искусственном интеллекте [12]. Основная цель принятия данного закона – это обеспечение того, чтобы системы ИИ, используемые в ЕС, были безопасными, прозрачными, отслеживаемыми, недискриминационными и экологически чистыми.

В настоящей же статье мы рассмотрим вопрос обеспечения цифрового суверенитета государства на примере ошибок ИИ обстоятельством непреодолимой силы.

По нашему мнению, одним из механизмов обеспечения государственного суверенитета может являться нормативное регулирование эксплуатации цифровых технологий, с помощью которых государство способно осуществлять регулирование общественных отношений, с целью прогнозирования, выявления и предотвращения угроз гражданскому обороту.

Регулирование института ИИ необходимо для его нормального применения в обороте. Непреодолимая сила же является той границей, которая позволяет участникам правоотношений прогнозировать пределы своей ответственности.

В настоящее время ИИ проник почти во сферы жизни общества: боевые машины, чаты, переводчики, автомобили, оказание медицинских услуг и т.д.

В рамках исследования проблемы обеспечения государственного суверенитета особо интересным является вопрос применения ИИ в военной промышленности.

Так, Albader F. в своей статье разбирает проблему несения государством ответственности за ошибку ИИ, допущенную при использовании современных систем вооружения, а также возможность применения в данном случае института непреодолимой силы [13]. В результате своего исследования автор приходит к выводу о невозможности распространения института непреодолимой силы в случае совершения ошибок ИИ в том случае, если речь идет об автономном оружии.

Однако выводы автора данной статьи отнюдь не бесспорны. Так, например, автор указывает, что материальная невозможность избежать последствий ошибки ИИ может быть связана с естественными событиями, такими как шторм или землетрясение, и/или вмешательством человека [13]. Исходя из данного аргумента можно заключить, что автор исследовал возможности так называемого «слабого искусственного интеллекта», без учета теоретических возможностей «сильного».

Таким образом, сделанные автором вышеуказанной работы выводы нуждаются в более глубоком исследовании с учетом деления ИИ на «сильный» и «слабый». Более того, вопрос исследовался автором также без учета наличия субъективного и объективного подходов к институту непреодолимой силы, что, по мнению авторов настоящей статьи, может существенно повлиять на результаты исследований.

Государство как участник данных правоотношений, в особенности в военной сфере, заинтересовано в их предсказуемости посредством обеспечения качественного нормативного регулирования данной сферы, а также глубокой проработке в области правового обеспечения использования ИИ. В ином случае, совершение ИИ в данной сфере деятельности государства может повлечь серьезные последствия для суверенитета государства в целом.

В заключении авторы настоящей работы делают вывод о том, что исследование концепции применения института непреодолимой силы в отношении ошибок ИИ, как одной из ключевых частей нормативного регулирования в данной сфере, является первоочередной задачей и требует привлечения внимания в научной литературе.

Глубокое исследование данного вопроса преследует целый комплекс различных задач, таких как: обеспечение цифрового суверенитета государства и стабильности оборота, внесение предсказуемости в вопросе привлечения к ответственности в тех сферах, в которых используется ИИ, а также позволит создать базу для дальнейшего нормативного регулирования в данной сфере. Именно данные факторы позволят обеспечить стабильное развитие государства в цифровой сфере, что обеспечивает его цифровой суверенитет в первую очередь. При исследовании данной проблемы особое место следует уделить таким категориям как «воля» и «ответственность», т.к. именно данные категории играют особую роль в обеспечении государственного контроля в цифровой сфере.

Список использованных источников:

1. Чердаков, О.И. Обеспечение безопасности социально-экономических институтов в связи с внедрением технологий искусственного интеллекта в России / О.И. Чердаков, С.Б. Куликов // Безопасность бизнеса. – 2022. – № 6. – С. 3–9.

2. Баранова, А.Ф. Цифровой суверенитет ЕАЭС в контексте обеспечения экономической безопасности / А.Ф. Баранова, Е.С. Шмагун // Государственная власть и местное самоуправление. – 2022. –№ 7. – С. 29–34.

3. Петроченков, И.А. К вопросу о концепции цифрового суверенитета / И.А. Петроченков // Конституционное и муниципальное право. – 2022. – № 7. С. 69–73.

4. Ефремов, А.А. Формирование концепции информационного суверенитета государства / А.А. Ефремов // Право: Журнал Высшей школы экономики. – 2017. – № 1. – С. 201–215.

5. Brokes, F. Russia's Sovereign Internet / F. Brokes // Central European Financial Observer. 2018. September 24. – Режим доступа: https://financialobserver.eu/cse-and-cis/russias-sovereign-internet/ – Дата доступа 01.10.2023.

6. Доктрина информационной безопасности Российской Федерации, утв. Указом Президента РФ, 5 дек. 2016 г., № 646 // СЗ РФ. – 2016. – № 50. – Ст. 7074.

7. О развитии искусственного интеллекта в Российской Федерации (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года) [Электронный ресурс]: Указ Президента РФ, 10 окт. 2019 г., № 490 // Кремлин. –Режим доступа: www.kremlin.ru/acts/bank/44731 – Дата доступа 08.10.2023.

8. Об Основных направлениях реализации цифровой повестки ЕАЭС до 2025 г. [Электронный ресурс]: решение Высшего евразийского экономического совета, 11 окт. 2017 г. №12 // Гарант. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/71708158/ – Дата доступа 01.10.2023.

9. Баранова, А.Ф. Цифровой суверенитет ЕАЭС в контексте обеспечения экономической безопасности / А.Ф. Баранова, Е.С. Шмагун // Государственная власть и местное самоуправление. – 2022. – № 7. – С. 29–34.

10. Рассолов, И.М. Информационное право в системе права: тенденции, перспективы становления и развития / И.М. Рассолов // Информационное право: актуальные проблемы теории и практики : сб. докладов Междунар. науч.-практ. конф., Москва, 7 апр. 2016 г. / ред. сов. Ю.Л. Васильченко, И.М. Рассолов, С.Г. Чубукова. – М. : МГЮА, 2016. – С. 5–9.

11. Анисимова, А.С. Интернет как фактор трансформации права в условиях развития цифровых технологий / А.С. Анисимова // Формирование системы правового регулирования обеспечения информационной безопасности в условиях больших вызовов в глобальной информационном обществе. Вторые Бачиловские чтения: Сб. науч. тр. / под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. – М. : ИГП РАН, 2019. – С. 202.

12. AI Rules: What The European Parliament Wants, Eur. Parliament. [Электронный ресурс] // Европейский парламент – Режим доступа: https://www.europarl.europa.eu/news/en/headlines/society/20201015STO89417/ai-rules-what-the-european-parliament-wants – Дата доступа 08.10.2023;

13. Fatemah Albader Exploring the Application of Force Majeure for AI Mistakes in Armed Conflict [Электронный ресурс] // Harvard National Security Journal. 2023. Jan. 29. –Режим доступа: https://harvardnsj.org/2023/01/29/exporing-the-application-of-force-majeure-for-ai-mistakes-in-armed-conflict/ – Дата доступа 08.10.2023.