



Научная статья

УДК 340.143:004.8

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

DOI: <https://doi.org/10.21202/jdtl.2023.17>

Подходы к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта: особенности и практическая применимость

Ольга Сергеевна Ерахтина

Пермский филиал Национального исследовательского университета «Высшая школа экономики»
г. Пермь, Российская Федерация

Ключевые слова

Искусственный интеллект, опасность, право, программное обеспечение, регулирование, рискориентированный подход, технологический подход, управление рисками, цифровая экономика, цифровые технологии

Аннотация

Цель: обзор сложившихся в науке подходов к регулированию отношений в сфере применения технологий искусственного интеллекта, выявление основных особенностей и ограничений применения рискориентированного и технологического подходов для определения направлений их дальнейшего развития.

Методы: методологическую основу исследования составляет совокупность методов научного познания, в том числе общенаучный диалектический и универсальные научные методы (анализ и синтез, сравнение, обобщение, структурно-функциональный, формально-логический).

Результаты: определено, что применение рискориентированного подхода предполагает построение конструктивных моделей управления рисками. Значимым вопросом для применения данного подхода является вопрос об основаниях отнесения технологий искусственного интеллекта к высокорисковым. При определении уровня риска применения технологии искусственного интеллекта необходимо применять следующие критерии: тип технологии искусственного интеллекта, сферу ее применения, а также уровень ее потенциальной опасности для окружающей среды, здоровья, других фундаментальных прав граждан.

В свою очередь, центральным вопросом для применения технологического подхода является вопрос о необходимости и пределах регулирования сферы разработки и применения технологий искусственного интеллекта. Во-первых, вмешательство в данную сферу не должно создавать препятствий для развития технологий и инноваций.

© Ерахтина О. С., 2023

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.

Во-вторых, естественная реакция регулятора в ответ на появление новых объектов и субъектов оборота – «синдром несовершенного закона». Вместе с тем ложное представление об отсутствии правового регулирования может дать обратный эффект – дублирование правовых норм. В целях решения проблемы дублирования законодательных требований следует прежде всего решить вопрос о том, необходимо ли регулировать технологии искусственного интеллекта или некоторые виды использования программного обеспечения.

Научная новизна: проведен обзор основных подходов к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта, выявлены возможности и ограничения их применения, предложены дальнейшие направления их развития.

Практическая значимость: основные положения и выводы исследования могут быть использованы для определения оптимальных подходов к регулированию сферы цифровых технологий, а также в целях совершенствования правового регулирования рассматриваемой области общественных отношений.

Для цитирования

Ерахтина, О. С. (2023). Подходы к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта: особенности и практическая применимость. *Journal of Digital Technologies and Law*, 1(2), 421–437. <https://doi.org/10.21202/jdtl.2023.17>

Содержание

Введение

1. Рискоориентированный подход

2. Технологический подход

Выводы

Список литературы

Введение

Активное развитие технологий и систем искусственного интеллекта порождает научные дискуссии о необходимости, пределах и задачах правового регулирования отношений в сфере ИТ. Учеными высказываются принципиально разные позиции: от утверждений о необходимости установления значительного количества обязательных требований, исполнение которых в большей степени возлагается на разработчика (Smuha, 2021), до предложений не осуществлять правовое вмешательство в сферу высоких технологий¹, чтобы не препятствовать инновациям. В палитру позиций ученых входят также более умеренные взгляды: применение международных и национальных стандартов (Zielke, 2020); осуществление добровольной сертификации (Ellul et al., 2021); мягкое регулирование и саморегулирование (Erdélyi & Goldsmith, 2018); установление объяснимых (Hamon et al., 2022) и этических (Wagner, 2018) рамок.

¹ O'Sullivan, Andrea. (2017, October 24). *Don't Let Regulators Ruin AI*. <https://www.technologyreview.com/2017/10/24/3937/dont-let-regulators-ruin-ai/>

Бельгийский исследователь Николя Пети предлагает так называемый регуляторный компромисс, достигаемый посредством соотношения угроз и возможностей, создаваемых введением правового регулирования². Он приводит ряд примеров, когда регулирование создавало препятствия для технологического процесса³. Вместе с тем отмечает, что отсутствие регулирования также может помешать технологической эволюции. В частности, правовая неопределенность оказывает негативное влияние на инвестиции. По мнению Райана Кало, неопределенные правила ответственности могут служить препятствием для инвестиций в открытые рынки робототехники и направить поток капитала на узкую функциональность роботов, где производители могут лучше управлять рисками, оставляя открытую робототехнику недостаточно развитой (Calo, 2011).

Среди множества подходов к правовому регулированию отношений в сфере применения систем искусственного интеллекта выделяют подход, согласно которому определяется общий правовой режим, который должен предусматривать основные требования к обеспечению безопасности систем искусственного интеллекта. Данный режим будет распространяться на все подобные системы. Наряду с этим необходимо разработать детальные требования к разработке и применению искусственного интеллекта в конкретных сферах (Понкин, Редькина, 2018).

Высокая динамика развития технологий искусственного интеллекта, наличие множества регуляторных инициатив актуализируют значимость междисциплинарных исследований, нацеленных на выявление оптимальных подходов к регулированию рассматриваемой сферы общественных отношений.

В статье представлен комплексный анализ двух междисциплинарных подходов к регулированию отношений в сфере разработки и применения технологий искусственного интеллекта – рискориентированного и технологического подходов, выявлены возможности и ограничения их применения, а также определены направления их дальнейшего развития.

1. Рискориентированный подход

Одним из активно обсуждаемых в науке подходов к регулированию технологий искусственного интеллекта является рискориентированный подход (Михалева, Шубина, 2019; Gellert, 2021; Gonçalves, 2020). Идея применения данного подхода была анонсирована в резолюции Европарламента «Нормы гражданского права в робототехнике» в 2017 г.⁴ Через четыре года в проекте Регламента Европейского союза, устанавливающего согласованные правила в отношении искусственного интеллекта⁵, была предложена классификация систем искусственного интеллекта, основанная

² Petit, N. (2017, March 9). *Law and Regulation of Artificial Intelligence and Robots – Conceptual Framework and Normative Implications* (Working paper, pp. 6–7). <http://dx.doi.org/10.2139/ssrn.2931339>

³ Там же. Р. 12.

⁴ European Parliament. (2017, February 15). *Draft Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))*. <https://www.europarl.europa.eu/portal/en>

⁵ European Parliament. (2021, April 21). *Regulation of the European Parliament and of the Council. Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts*. <https://www.europarl.europa.eu/portal/en>

на оценке уровня риска их применения. В соответствии с данной классификацией системы искусственного интеллекта разделены на четыре группы:

1) системы искусственного интеллекта с неприемлемо высоким уровнем риска (прежде всего, системы искусственного интеллекта, применяемые в военном и оборонном секторах, а также системы для манипулирования поведением человека и системы для создания социальных рейтингов);

2) системы искусственного интеллекта с высоким уровнем риска⁶;

3) системы искусственного интеллекта с ограниченным риском⁷;

4) системы искусственного интеллекта с минимальным риском⁸.

Для оценки уровня риска применения системы искусственного интеллекта предполагается использование двух основных критериев: степень зависимости пользователей от решений, которые принимает система, и степень ее опасности для жизни и здоровья граждан и нарушения их основных прав.

В проекте Регламента ЕС указывается на необходимость установления запрета на производство и введение в гражданский оборот систем искусственного интеллекта, применение которых создает неприемлемо высокий уровень риска причинения вреда. В свою очередь к разработчикам, владельцам и пользователям высокорисковых систем искусственного интеллекта, как следует из проекта, должны предъявляться повышенные требования к обеспечению безопасности, ведению технической документации и предоставлению информации⁹. В целях соблюдения установленных требований могут быть использованы системы менеджмента качества. Для систем же с ограниченным и минимальным риском как минимум должна быть установлена обязанность информировать пользователей о том, что они взаимодействуют с искусственным интеллектом.

В целом подход ЕС заслуживает поддержки. Вместе с тем он нуждается в дальнейшем развитии.

Во-первых, необходимо учитывать, что рискориентированный подход – это система управления рисками, которая состоит из трех основных этапов. На первом этапе необходимо выявить, проанализировать и дифференцировать прогнозируемые риски. На втором – провести оценку уровня риска. На третьем этапе – определить способы управления рисками.

При всем многообразии подходов к классификации рисков (в идеале все эти подходы должны быть обязательно учтены) для целей данной статьи можно выделить:

- внутренние и внешние риски;
- системные и несистемные риски.

⁶ Например, роботы-ассистенты в хирургии, управление и эксплуатация критической инфраструктурой.

⁷ Например, чат-боты, виртуальные помощники, умные дома.

⁸ Например, видеоигры, спам-фильтры.

⁹ При разработке и применении таких систем должны соблюдаться «принципиальные требования», такие как требования к качеству данных, документированию и прослеживаемости, человеческому контролю и др. В частности, до размещения на рынке или введения в эксплуатацию должна быть составлена техническая документация, в которой необходимо отразить соответствие системы установленным требованиям, а также всю необходимую информацию для оценки системы на соответствие (статья 11). Проект также требует разрабатывать системы таким образом, чтобы обеспечивались ведение учета во время работы системы (статья 12), а также прозрачность системы ИИ и предоставление информации (статья 13), с тем чтобы пользователи высокорисковых систем могли использовать их надлежащим образом и корректно интерпретировать выходные данные. Контроль со стороны человека должен осуществляться на протяжении всего жизненного цикла системы с возможностью в любой момент вмешаться в работу системы и при необходимости остановить или скорректировать ее.

Внутренние риски возникают в отдельно взятой компании, их можно спрогнозировать, оценить и предотвратить своими силами. Внешние риски (изменение экономической и политической ситуации, стихийные бедствия, экологические катастрофы и др.) предотвратить силами отдельной компании нельзя.

Системные риски угрожают рынку в целом или отдельным сферам бизнеса. Спрогнозировать их возникновение и оценить последствия могут только эксперты. Их также нельзя предотвратить силами отдельной компании. В то время как несистемные (коммерческие) риски – это риски отдельной компании, которые она может и должна минимизировать самостоятельно.

Концепция рискориентированного подхода в понимании резолюции Европарламента «Нормы гражданского права в робототехнике» направлена на управление внутренними и несистемными рисками и оставляет без внимания внешние и системные риски, которые не могут быть вменены отдельным субъектам гражданского оборота. Выявление таких рисков – это одна из основных задач, которая должна быть решена на первом этапе.

На втором этапе определяется уровень риска (вероятность материализации риска и размер неблагоприятных последствий, которые могут вследствие этого наступить). На первый взгляд, проект решает данную задачу. Вместе с тем основания для отнесения системы искусственного интеллекта к одной из четырех групп требуют дальнейшего исследования. Как уже было указано, в проекте Регламента предлагается в качестве критерия оценки уровня риска использовать степень зависимости пользователей от решений, которые принимает искусственный интеллект, и степень опасности технологии для жизни и здоровья граждан и нарушения их основных прав. На наш взгляд, оценка вероятности материализации риска зависит и от ряда других факторов. Прежде всего, это характеристики технологии. Основными характеристиками искусственного интеллекта являются его автономность (способность самостоятельно, без вмешательства человека принимать решения) и обучаемость (способность овладевать новыми навыками и способностями). При этом в зависимости от сферы применения выделяют несколько уровней автономности технологий. Так, в Приложении № 10 к Транспортной стратегии РФ до 2030 г. с прогнозом на период до 2035 г.¹⁰ определено пять уровней автономности автомобильного транспорта, четыре уровня автономности железнодорожного транспорта и шесть уровней автономности водного и морского транспорта.

По критерию обучаемости искусственный интеллект может быть необучаемым, обучаемым и самообучаемым. Очевидно, что высокоавтономные и самообучаемые технологии должны быть отнесены к высокорисковым системам искусственного интеллекта, а необучаемые, имеющие первый или второй уровень автономности, – к системам с минимальным риском. Однако решение задачи определения уровня риска применения технологии искусственного интеллекта на основе ее характеристики не является настолько простой, насколько может показаться на первый взгляд. Прежде всего потому, что при оценке риска наряду с автономностью и способностью к обучению необходимо учитывать и другие характеристики искусственного интеллекта. В частности, функциональность (способность выполнять одну или более функций) технологии, оснащенность средствами контроля (Алексеев и др., 2020). Кроме того, очевидно, что возможны различные комбинации

¹⁰ Утверждена распоряжением Правительства РФ от 27.11.2021 № 3363-р. <https://base.garant.ru/403156321/>

указанных характеристик. Так, например, технология искусственного интеллекта может быть высокоавтономной, обучаемой, выполняющей две функции и не содержать средства объективного контроля.

В научных работах также предлагается в качестве критерия оценки риска применения технологий искусственного интеллекта учитывать сферу их применения. По мнению группы исследователей из Мальтийского университета, правовое регулирование должно быть обязательным только для критических областей и сфер деятельности. При этом наряду со сферой применения систем искусственного интеллекта необходимо проводить оценку уровня риска тех видов деятельности, при осуществлении которых он используется (Ellul et al., 2021). С данным выводом следует согласиться. Так, в сфере здравоохранения технологии искусственного интеллекта могут применяться для помощи врачам при постановке диагноза, назначении лекарственных препаратов, проведении операций. Указанные виды деятельности могут быть отнесены к категории высокого риска. Наряду с этим технологии искусственного интеллекта используются для регистрации пациентов, обработки и анализа медицинских данных, автоматического оповещения медицинского персонала. Представляется, что данные виды деятельности могут быть отнесены к группе ограниченного риска.

Сферу транспорта большинство авторов также относят к высокорисковой сфере. Однако и здесь необходимо учитывать, для сопровождения каких видов деятельности применяется искусственный интеллект. Системы искусственного интеллекта используются для повышения безопасности и эффективности транспортного процесса, управления пассажиропотоками и грузовыми потоками. Вместе с тем технологии искусственного интеллекта также используются при оказании услуг по перевозке грузов и пассажиров. Если деятельность по управлению транспортной инфраструктурой относится к категории высокого риска, то деятельность по оказанию услуг может быть отнесена к категории ограниченного риска.

Во-вторых, в дальнейших исследованиях нуждается и вопрос о способах управления рисками. Проект уделяет основное внимание высокорисковым системам, оставляя, по сути, без внимания системы искусственного интеллекта с ограниченным риском. Вместе с тем специальное регулирование (основанное на рискориентированном подходе) должно в том числе осуществляться и применительно к системам искусственного интеллекта, относящимся к данной группе.

Полагаем, что способы управления рисками будут различаться в зависимости от вида риска (внутренний или внешний, системный или несистемный), а также уровня «рисковости» технологии искусственного интеллекта (высокий или средний).

Заслуживающей внимания является «Базовая модель определения критериев и категорий риска», утвержденная в 2017 г. проектным комитетом приоритетной программы «Реформа контрольной и надзорной деятельности»¹¹. В данном документе раскрываются такие понятия, как «источники риска», «факторы риска», «профиль риска», определяются их виды, предлагаются способы ранжирования управляемых факторов и профилей риска (в целях определения наиболее значимых из них)

¹¹ «Базовая модель определения критериев и категорий риска» (утв. протоколом заседания проектного комитета от 31.03.2017 № 19(3)) (вместе с «Требованиями к обоснованию предлагаемых федеральными органами исполнительной власти – участниками приоритетной программы “Реформа контрольной и надзорной деятельности” категорий риска (классов опасности) и критериев риска в отношении осуществляемых ими видов государственного контроля (надзора)»).

и методика определения величины причиняемого вреда и возможной частоты возникновения потенциальных негативных последствий.

Несмотря на то, что рассматриваемая модель была принята в целях осуществления надзорными органами «умных проверок», чтобы сконцентрировать проверки на потенциально наиболее опасных объектах, предлагаемые в нем методики определения категорий и критериев риска могут быть использованы и при оценке уровня риска применения технологий искусственного интеллекта.

2. Технологический подход

В последнее время в научной литературе все большее внимание уделяется технологическому подходу, в центре внимания которого находятся сама технология, ее сущностные и специфические характеристики. Рассматривая развитие технологии и инноваций в качестве основной задачи правового регулирования, представители данного подхода прежде всего задаются вопросом о необходимости и пределах регулирования сферы высоких технологий. Размышляя над этим вопросом, Дж. Эллул, приходит к выводу о том, что правовое регулирование должно быть сосредоточено не на искусственном интеллекте, а на программном обеспечении. По его мнению, в случае критического программного обеспечения, используемого, например, в самолете, не имеет значения, используется ли при этом искусственный интеллект или нет. Регулирование не должно касаться конкретной технологии искусственного интеллекта, оно должно быть более широким и осуществляться в отношении программного обеспечения в целом. В подтверждение данного вывода Эллул приводит еще один пример. Так, при использовании искусственного интеллекта в банковских или страховых системах, которые решают, следует ли предлагать конкретный кредит или полис, регулирование должно быть направлено на обеспечение того, чтобы клиенты не подвергались дискриминации. Данное требование должно применяться не только к системам на основе искусственного интеллекта. Вполне возможно запрограммировать систему для принятия решений, используя методы, не связанные с искусственным интеллектом (Ellul, 2022).

В целом поддерживая данную точку зрения, необходимо учитывать, что искусственный интеллект является собирательным понятием. В нормативно-правовых актах обоснованно проводится последовательное разграничение понятий «программа для ЭВМ»¹², «искусственный интеллект»¹³ и «технологии искусственного интеллекта»¹⁴.

¹² Статья 1261 Гражданского кодекса РФ.

¹³ Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», которым утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 г.

¹⁴ Статья 2 Федерального закона от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных».

В примечании к п. 3.18 Национального стандарта «Системы искусственного интеллекта. Классификация систем искусственного интеллекта»¹⁵ указано на то, что искусственный интеллект как комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения), процессы и сервисы по обработке данных, анализу и синтезу решений.

В научной литературе также поднимается вопрос о том, является ли искусственный интеллект единым объектом либо это собирательное понятие (Балашова, 2022). В качестве решения данного вопроса Л. Ю. Василевской предлагается включить искусственный интеллект в установленный в ст. 1240 ГК РФ перечень сложных объектов интеллектуальных прав. По мнению, Л. Ю. Василевской, структурными элементами искусственного интеллекта являются программный продукт (программа для ЭВМ); программное обеспечение (совокупность программ); искусственные нейронные сети (программы для ЭВМ); алгоритмы, программное обеспечение в качестве ноу-хау; технические решения как изобретения; базы данных (Василевская и др., 2021).

Таким образом, несмотря на то, что ядром технологии искусственного интеллекта является компьютерная программа, полностью отождествлять эти понятия было бы неверным. Именно отличительные особенности систем искусственного интеллекта, их специфические характеристики и наличие структурных элементов, являющихся самостоятельными объектами гражданских прав, обуславливают особенности правового регулирования отношений в сфере их разработки и применения.

Применение технологического подхода призвано также не допустить дублирования законодательных требований в тех сферах, где они уже введены. В этой связи Дж. Эллул ставит еще один исследовательский вопрос: должно ли, например, программное обеспечение для планирования задач в календаре регулироваться в большей степени, чем того требуют существующие законы (например, Закон о защите персональных данных или Закон о защите прав потребителей) (Ellul, 2022)? Полагаю, что на данный вопрос следует ответить утвердительно. Развитие технологий меняет процесс взаимодействия участников оборота, а соответственно, содержание их прав и обязанностей. Так, ст. 12 Закона о защите прав потребителей устанавливает обязанность изготовителя (исполнителя, продавца) своевременно предоставлять потребителю необходимую и достоверную информацию о товарах (работах, услугах). Вместе с тем в цифровом обществе информация, как правило, предоставляется в цифровой форме. Наряду с этим появляются программы, облегчающие поиск информации. А. И. Савельев справедливо отмечает, что в перспективе на потребителя, по-видимому, будет возложен риск неознакомления с информацией, размещенной предпринимателем в общедоступных источниках (Савельев, 2016). Более того, законодатель вводит в гражданский оборот новых субъектов. Так, в июле 2018 г. Законом «О внесении изменений в Закон Российской Федерации «О защите прав потребителей»¹⁶ было установлено специальное регулирование деятельности владельца агрегатора информации о товарах (услугах).

¹⁵ ГОСТ Р 59277-2020. Национальный стандарт РФ. Системы искусственного интеллекта. Классификация систем искусственного интеллекта. Дата введения 01.03.2021.

¹⁶ О внесении изменений в Закон Российской Федерации «О защите прав потребителей»: Федеральный закон от 29.07.2018 № 250-ФЗ. http://www.consultant.ru/document/cons_doc_LAW_303537/

Применение технологий искусственного интеллекта при обработке и хранении персональных данных связано с рисками их утечки или некорректной интерпретации. С 1995 г. Европейский парламент решает проблему управления такими рисками¹⁷. В 2016 г. в Регламенте ЕС «О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных» была предложена модель, призванная решить задачу усиления защиты персональных данных. Применение данной модели, по мнению разработчиков Регламента, должно способствовать формированию доверительного отношения к технологиям¹⁸.

И, наконец, последний вопрос, который исследует Эллул в своей статье: должно ли обязательное регулирование быть ориентировано непосредственно на технологии либо на определенную сферу или вид деятельности, при осуществлении которой они применяются (Ellul, 2022)? При ответе на данный вопрос необходимо учитывать, что риск ошибки имманентно присущ программному обеспечению любой сложности, вне зависимости от того, обладает оно элементами искусственного интеллекта или нет. По мере того, как программные системы в целом (которые не обязательно используют искусственный интеллект) «растут в сложности, взаимосвязанности и географическом распределении, мы будем все чаще сталкиваться с их нежелательным эмерджентным поведением» (Mogul, 2006). То есть взаимодействие технологии с внешней средой создает дополнительные сложности и риски. В целях минимизации таких рисков прежде всего необходимо вводить стандарты качества программного обеспечения¹⁹. Затем необходимо проводить оценку уровня риска тех видов деятельности, при осуществлении которых используется технология (об этом мы писали в первой части нашей статьи). Если определенная деятельность относится к группе высокого риска, должно быть установлено требование обязательного применения соответствующего стандарта. Таким образом, обязательное регулирование должно быть ориентировано не на технологию, а на вид деятельности, при осуществлении которой она применяется.

Рассматривая основные вопросы, которые поднимаются представителями технологического подхода, нельзя оставить без внимания исследование Рональда Линса. Исследователь из Нидерландов указывает на то, что выявить наличие пробелов в правовом регулировании отношений в сфере применения технологий – это достаточно сложная задача. На первом этапе необходимо определить сущностные и специфические характеристики технологии. Следует ли при решении этой задачи сосредоточиться на конкретном примере технологии, например на беспилотных автомобилях, или перейти к более широкой категории – беспилотным транспортным средствам?

¹⁷ О защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных: Директива ЕС 95/46/ЕС от 24 октября 1995 г. (Директива ЕС 95/46/ЕС «О персональных данных»).

¹⁸ О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных: Регламент ЕС 2016/679 от 27 апреля 2016 г.

¹⁹ См., например: ГОСТ 28195-89. Оценка качества программных средств. Общие положения. Введен 01.07.1990; ГОСТ 28806-90. Качество программных средств. Термины и определения. Введен 01.01.1992; ГОСТ Р 51188-98. Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство. Введен 01.07.1999.

По мнению Линса, ни один из этих подходов не является желательным. Фокусирование на определенной технологии может привести к тому, что регулятор сосредоточится на потенциально случайных особенностях технологии. Во втором случае из-за чрезмерного обобщения дискуссия может стать абстрактной, а потому бесполезной. Поэтому на данном этапе надо взять «социально-техническую призму» и наряду с определением специфических характеристик технологии выявить, чьи интересы должны быть важны и приоритетны (Leenes, 2019).

На втором этапе необходимо решить вопрос развития технологий, для чего выявить потенциальные риски и существующие проблемы, с которыми связано их применение. К сожалению, в научной литературе очень часто происходит смешение таких категорий, как «риск» и «проблема», в связи с чем сложно четко определить пределы и задачи правового регулирования рассматриваемой сферы общественных отношений. Представляется, что одним из основных рисков применения технологий искусственного интеллекта является возможность ее самопроизвольного отклонения от изначально заложенной в ней цели. Вследствие материализации данного риска возможно наступление определенных негативных последствий, таких как причинение вреда жизни, здоровью или имуществу пользователя, разглашение конфиденциальной информации.

На необходимость разграничения категорий «риск» и «проблема» указывают Е. А. Войниканис, Е. В. Семенова, Г. С. Тюляев. К рискам применения технологий искусственного интеллекта они, в частности, относят возможность деанонимизации данных, возможность дискриминации по признакам пола, расы, национальности, вероисповедания. В качестве проблем в работе выделяются вопросы о том, кто является правообладателем программы искусственного интеллекта, кто является ответственным за причинение вреда жизни или здоровью при эксплуатации искусственного интеллекта, и др. (Войниканис и др., 2018).

На третьем этапе следует определить формы и пределы государственного вмешательства в сферу технологий искусственного интеллекта. Способы управления рисками и решения проблем минимизации негативных последствий их материализации различны. Так, например, к способам управления рисками можно отнести ведение регистрационного журнала во время работы системы, а также обеспечение прозрачности процесса принятия решения, чтобы пользователи могли интерпретировать выходные данные. В отношении высокорисковых систем должна быть также введена система пострыночного мониторинга, в рамках которого будут осуществляться сбор и анализ данных о работе системы уже после ее вывода на рынок.

Если же, несмотря на принятие превентивных мер контроля, произошел сбой в работе системы, право должно предоставить способы справедливого распределения негативных последствий между ее разработчиком, пользователем и оператором.

Необходимо также учитывать, что способы воздействия на риски и проблемы различны и не всегда имеют правовую форму. При этом, по справедливому замечанию М. Шерера (Scherer, 2016), традиционные методы правового регулирования, такие как, например, лицензирование продукции, контроль за исследованиями, возможность применения деликтной ответственности, являются не вполне пригодными для управления рисками, связанными с применением систем искусственного интеллекта.

Выводы

Применение рискориентированного подхода предполагает построение конструктивных моделей управления рисками. Процесс управления рисками состоит из трех основных этапов. На первом этапе необходимо выявить и классифицировать все риски, с которыми сопряжено применение технологий искусственного интеллекта в определенной сфере. Концепция рискориентированного подхода, предлагаемая Европарламентом, концентрируется на внутренних и несистемных рисках. Соответственно, в целях развития данного подхода необходимо провести исследование по выявлению внешних и системных рисков. На втором этапе необходимо провести оценку уровня риска применения определенной технологии искусственного интеллекта. При проведении оценки необходимо использовать ряд критериев. Среди них – сущностные и специфические характеристики технологии, сфера и вид деятельности, при осуществлении которой применяется данная технология. На третьем этапе должны быть определены способы управления рисками, которые в свою очередь дифференцируются в зависимости от уровня рисковости определенной технологии. Как видим, основная цель применения рискориентированного подхода состоит в определении способов управления рисками, с которыми сопряжено применение технологий искусственного интеллекта.

В центре внимания технологического подхода находится вопрос о необходимости и пределах регулирования сферы высоких технологий. К основным этапам применения технологического подхода относят:

- определение сущностных и специфических характеристик технологий;
- выявление потенциальных рисков и уже существующих проблем их применения;
- определение форм и пределов государственного вмешательства в сферу технологий искусственного интеллекта.

Именно специфические характеристики технологий искусственного интеллекта, такие как автономность и самообучаемость, обуславливают особенности правового регулирования отношений в сфере их разработки и применения. При этом обязательное регулирование должно быть ориентировано не на технологию, а на вид деятельности, при осуществлении которой она применяется.

Проведенное исследование позволяет также сделать вывод о том, что универсальным подходом к регулированию отношений в сфере разработки и применения технологий является технологический подход. Несмотря на то, что данный подход нуждается в дальнейшем развитии, уже сейчас он может послужить основой для формирования стратегии правотворческой деятельности. В свою очередь, рискориентированный подход является одним из основных элементов технологического подхода. Эффективное управление сопутствующими рисками позволит минимизировать потенциальные негативные последствия применения новых технологий и обеспечит устойчивое развитие сферы высоких технологий.

Список литературы

- Алексеев, А. О., Ерахтина, О. С., Кондратьева, К. С., Никитин, Т. Ф. (2020). Подходы к гражданско-правовой ответственности разработчика технологий искусственного интеллекта: на основе классификации технологий. *Информационное общество*, 6, 47–57. <https://elibrary.ru/ylddab>
- Балашова, А. И. (2022). Искусственный интеллект в авторском и патентном праве: объекты, субъектный состав правоотношений, сроки правовой охраны. *Журнал Суда по интеллектуальным правам*, 2(36), 90–98. <https://elibrary.ru/apldua>

- Василевская, Л. Ю., Подузова, Е. Б., Тасалов, Ф. А. (2021). Цифровизация гражданского оборота: правовая характеристика «искусственного интеллекта» и «цифровых» субъектов (цивилистическое исследование) (в 5 т.). Москва: Проспект. <https://elibrary.ru/nrjkdo>
- Войниканис, Е. А., Семенова, Е. В., Тюляев, Г. С. (2018). Искусственный интеллект и право. Вызовы и возможности самообучающихся алгоритмов. *Вестник Воронежского государственного университета. Серия: Право*, 4(35), 137–148. <https://elibrary.ru/yumlhz>
- Михалева, Е. С., Шубина, Е. А. (2019). Проблемы и перспективы правового регулирования робототехники. *Актуальные проблемы российского права*, 12(109), 26–35. <https://doi.org/10.17803/1994-1471.2019.109.12.026-035>
- Понкин, И. В., Редькина, А. И. (2018). Искусственный интеллект с точки зрения права. *Вестник РУДН. Серия: Юридические науки*, 22(1), 91–109. <https://doi.org/10.22363/2313-2337-2018-22-1-91-109>
- Савельев, А. И. (2016). Направления эволюции свободы договора под влиянием современных информационных технологий. В сб. М. А. Рожкова (рук. авт. кол. и отв. ред.), *Свобода договора*. Москва: Статут. <https://elibrary.ru/xxoolt>
- Calo, R. (2011). Open robotics. *Maryland Law Review*, 70.3, 101–142.
- Ellul, J., Pace, G., McCarthy, S., Sammut, T., Brockdorf, J., & Scerri, M. (2021). Regulating artificial intelligence: a technology regulator's perspective. In *Proceedings of the Eighteenth International conference on artificial intelligence and law* (pp. 190–194). <https://doi.org/10.1145/3462757.3466093>
- Ellul, J. (2022). Should we regulate Artificial Intelligence or some uses of Software? *Discover Artificial Intelligence*, 2(5). <https://doi.org/10.1007/s44163-022-00021-9>
- Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society* (pp. 95–101).
- Gellert, R. (2021). The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? *Journal of Ethics and Legal Technologies*, 3(2), 15–33.
- Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*, 23(2), 139–152. <https://doi.org/10.1080/13669877.2018.1517381>
- Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE Comput Intell Mag.*, 17(1), 72–85. <https://doi.org/10.1109/mci.2021.3129960>
- Leenes, R. (2019). *Regulating New Technologies in Uncertain Times*. https://doi.org/10.1007/978-94-6265-279-8_2
- Mogul, J. C. (2006). Emergent (mis) behavior vs. complex software systems. *ACM SIGOPS Oper. Syst. Rev.*, 40(4), 293–304. <https://doi.org/10.1145/1218063.1217964>
- Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353–400. <https://doi.org/10.2139/ssrn.2609777>
- Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. *Law. Innov. Technol.*, 13(1), 57–84. <https://doi.org/10.1080/17579961.2021.1898300>
- Wagner, B. (2018). Ethics as an escape from regulation: from ethics-washing to ethics-shopping. In *Being profiling: cogitas ergo sum* (pp. 86–90). Amsterdam: Amsterdam University Press. <https://doi.org/10.1515/9789048550180-016>
- Zielke, T. (2020). Is artificial intelligence ready for standardization? In *European conference on software process improvement* (pp. 259–274). Springer.

Сведения об авторе



Ерахтина Ольга Сергеевна – кандидат юридических наук, доцент, доцент кафедры гражданского и предпринимательского права, Пермский филиал Национального исследовательского университета «Высшая школа экономики»

Адрес: 614070, Российская Федерация, г. Пермь, ул. Студенческая, 38

E-mail: oerahtina@hse.ru

ORCID ID: <https://orcid.org/0000-0002-9041-3487>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/K-3149-2014>

Google Scholar ID: <https://scholar.google.ru/citations?hl=ru&user=WdwWB4kAAAAJ>

РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=498773

Конфликт интересов

Автор заявляет об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

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: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 10 февраля 2023 г.

Дата одобрения после рецензирования – 23 апреля 2023 г.

Дата принятия к опубликованию – 16 июня 2023 г.

Дата онлайн-размещения – 20 июня 2023 г.



Research article

DOI: <https://doi.org/10.21202/jdtl.2023.17>

Approaches to Regulating Relations in the Sphere of Developing and Using the Artificial Intelligence Technologies: Features and Practical Applicability

Olga S. Erahtina

Perm branch of National Research University "Higher School of Economics"
Perm, Russian Federation

Keywords

Artificial intelligence,
danger,
digital economy,
digital technologies,
law,
regulation,
risk management,
risk-oriented approach,
software,
technological approach

Abstract

Objective: to review the modern scientific approaches to regulating relations in the sphere of using the artificial intelligence technologies; to reveal the main features and limitations of using the risk-oriented and technological approaches in order to determine the directions of their further development.

Methods: the methodological basis of the research is a set of scientific cognition methods, including the general scientific dialectic method and the universal scientific methods (analysis and synthesis, comparison, summarization, structural-functional, and formal-logical methods).

Results: it was determined that the use of the risk-oriented approach implies building constructive models of risk management. A significant issue in using this approach is the bases of referring the artificial intelligence technologies to high-risk ones. When determining the risk level of using the artificial intelligence technologies, the following criteria should be applied: the type of artificial intelligence technology, its sphere of use, and the level of potential harm for the environment, health and other fundamental human rights.

In turn, the central issue of using the technological approach is the necessity and limits of regulation in the sphere of developing and using the artificial intelligence technologies. First, interference into this sphere must not create obstacles for developing technologies and innovations. Second, a natural reaction of a regulator towards newly emerging objects and subjects of turnover is the "imperfect law syndrome". At the same time, a false idea

© Erahtina O. S., 2023

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.

about a lack of legal regulation may produce an opposite effect – duplication of legal norms. To solve the problem of duplicating legal requirements, it is necessary, first of all, to solve the issue of the need to regulate the artificial intelligence technologies or certain types of software applications.

Scientific novelty: a review was carried out of the main approaches to regulating relations in the sphere of developing and using the artificial intelligence technologies; the opportunities and limitations of their use are revealed; further directions of their development are proposed.

Practical significance: the main provisions and conclusions of the research can be used for determining the optimal approaches to regulating the sphere of digital technologies and for improving the legal regulation of the studied sphere of social relations.

For citation

Erahtina, O. S. (2023). Approaches to Regulating Relations in the Sphere of Developing and Using the Artificial Intelligence Technologies: Features and Practical Applicability. *Journal of Digital Technologies and Law*, 1(2), 421–437. <https://doi.org/10.21202/jdtl.2023.17>

References

- Alekseev, A. O., Erahtina, O. S., Kondratyeva K. S., & Nikitin, T. Ph. (2020). Approaches to civil legal liability of the artificial intelligence technologies developer: based on the classification. *Information Society*, 6, 47–57. (In Russ.).
- Balashova, A. I. (2022). Artificial intelligence in copyright and patent law: objects, subject structure of legal relations, terms of legal protection. *Zhurnal Suda po intellektual'nym pravam*, 2(36), 90–98. (In Russ.).
- Calo, R. (2011). Open robotics. *Maryland Law Review*, 70.3, 101–142.
- Ellul, J., Pace, G., McCarthy, S., Sammut, T., Brockdorf, J., & Scerri, M. (2021). Regulating artificial intelligence: a technology regulator's perspective. In: *Proceedings of the Eighteenth International conference on artificial intelligence and law* (pp. 190–194). <https://doi.org/10.1145/3462757.3466093>
- Ellul, J. (2022). Should we regulate Artificial Intelligence or some uses of Software? *Discover Artificial Intelligence*, 2(5). <https://doi.org/10.1007/s44163-022-00021-9>
- Erdélyi, O. J., & Goldsmith, J. (2018). Regulating artificial intelligence: proposal for a global solution. In *Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society* (pp. 95–101).
- Gellert, R. (2021). The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? *Journal of Ethics and Legal Technologies*, 3(2), 15–33.
- Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research*, 23(2), 139–152. <https://doi.org/10.1080/13669877.2018.1517381>
- Hamon, R., Junklewitz, H., Sanchez, I., Malgieri, G., & De Hert, P. (2022). Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. *IEEE ComputIntell Mag.*, 17(1), 72–85. <https://doi.org/10.1109/mci.2021.3129960>
- Leenes, R. (2019). *Regulating New Technologies in Uncertain Times*. https://doi.org/10.1007/978-94-6265-279-8_2
- Mikhaleva, E. S., & Shubina, E. A. (2019). Challenges and Prospects of the Legal Regulation of Robotics. *Actual Problems of Russian Law*, 1(12), 26–35. (In Russ.). <https://doi.org/10.17803/1994-1471.2019.109.12.026-035>
- Mogul, J. C. (2006). Emergent (mis)behavior vs. complex software systems. *ACM SIGOPS Oper. Syst. Rev.*, 40(4), 293–304. <https://doi.org/10.1145/1218063.1217964>
- Ponkin, I. V., & Redkina, A. I. (2018). Artificial Intelligence from the Point of View of Law. *RUDN Journal of Law*, 22(1), 91–109. (In Russ.). <https://doi.org/10.22363/2313-2337-2018-22-1-91-109>

- Savelyev, A. I. (2016). Directions of freedom of contract evolution under the influence of modern information technologies. In M. A. Rozhkova (head of authors' collective and editor-in-chief), *Svoboda dogovora*. Moscow: Statut. (In Russ.).
- Scherer, M. U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, 29(2), 353–400. <https://doi.org/10.2139/ssrn.2609777>
- Smuha, N. A. (2021). From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. *Law. Innov. Technol.*, 13(1), 57–84. <https://doi.org/10.1080/17579961.2021.1898300>
- Vasilevskaya, L. Yu., Poduzova, E. B., & Tasalov, F. A. (2021). *Digitalization of civil turnover: legal characteristics of "artificial intelligence" and "digital" subjects (civilistic research)* (In 5 Vol.). Moscow: Prospekt. (In Russ.).
- Voinikanis, E. A., Semenova, E. V., & Tyulyaev, G. S. (2018). Artificial intelligence and law: challenges and possibilities of self-learning algorithms. *Proceedings of Voronezh State University. Series: Pravo*, 4(35), 137–148. (In Russ.).
- Wagner, B. (2018). Ethics as an escape from regulation: from ethics-washing to ethics-shopping. In *Being profiling: cogitas ergo sum* (pp. 86–90). Amsterdam: Amsterdam University Press. <https://doi.org/10.1515/9789048550180-016>
- Zielke, T. (2020). Is artificial intelligence ready for standardization? In: *European conference on software process improvement* (pp. 259–274). Springer.

Author information



Olga S. Erahtina – Candidate of Sciences in Jurisprudence, Associate Professor, Department of Civil and Entrepreneurial Law, Perm branch of National Research University "Higher School of Economics"

Address: 38 Studencheskaya Str., 614070 Perm, Russian Federation

E-mail: oerahtina@hse.ru

ORCID ID: <https://orcid.org/0000-0002-9041-3487>

Web of Science Researcher ID:

<https://www.webofscience.com/wos/author/record/K-3149-2014>

Google Scholar ID: <https://scholar.google.ru/citations?hl=ru&user=WdwWB4kAAAAJ>

RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=498773

Conflict of interests

The author declares no conflict of interests.

Financial disclosure

The research was not sponsored.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – February 10, 2023

Date of approval – April 23, 2023

Date of acceptance – June 16, 2023

Date of online placement – June 20, 2023