ISSN 2949-2483

Volume 1 Number 4

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2023

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Том 1, № 4
2023
DOI: 10.21202/2949-2483.2023.4

ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

eISSN 2949-2483

Издается с 2023 года, периодичность – 4 выпуска в год. DOI: 10.21202/2949-2483

Редакционная коллегия

Редакция

Адрес: 420111, Российская Федерация, г. Казань, ул. Московская, 42
Телефон: +7 (843) 231-92-90
Факс: +7 (843) 292-61-59
E-mail: lawjournal@ieml.ru
Сайт: https://www.lawjournal.digital
Телеграм: https://t.me/JournalDTL
ВКонтакте: https://vk.com/JournalDTL
Яндекс.Дзен: https://dzen.ru/JournalDTL
Одноклассники: https://ok.ru/JournalDTL

Учредитель и издатель

Казанский инновационный университет имени В. Г. Тимирясова. Адрес: 420111, Российская Федерация, г. Казань, ул. Московская, 42. Телефон: +7 (843) 231-92-90. Факс: +7 (843) 292-61-59. E-mail: info@ieml.ru. Сайт: https://ieml.ru

Дата подписания к публикации – 30 ноября 2023 г. Дата онлайн-размещения на сайте https://www.lawjournal.digital – 15 декабря 2023 г.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 1, № 4
2023
DOI: 10.21202/2949-2483.2023.4
ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
eISSN 2949-2483

Содержание

Научная статья
УДК 34:004:349.3:364.23
EDN: https://elibrary.ru/aoqmxu
DOI: https://doi.org/10.21202/jdtl.2023.37

Цифровая инклюзия для людей с расстройствами аутистического спектра: пересмотр существующих правовых моделей и доктринальных концепций

Джеймс Хатсон ✉

Университет Линденвуд
г. Сент-Чарльз, США

Пайпер Хатсон

Университет Линденвуд
г. Сент-Чарльз, США

Ключевые слова

аутизм,
доступная среда,
законодательство,
инвалидность,
право,
расстройство аутистического спектра,
социальное обеспечение,
цифровая доступность,
цифровая инклюзия (инклюзивность),
цифровые технологии

Аннотация

Цель: в современном мире значительная доля профессиональных задач выполняется в цифровой среде, на цифровых площадках, в виртуальных и прочих собраниях, что обусловливает необходимость критического осмысления традиционных взглядов на проблему доступной среды и цифровой доступности с учетом базовых общечеловеческих потребностей инвалидов.

Методы: разрыв между традиционной правовой точкой зрения на особые условия труда для инвалидов и насущными потребностями «цифрового рабочего места» (цифровой среды) ярко показывает пробелы в понимании концепции доступности, которые выявляются и исследуются посредством формально-юридического и доктринального методов. Многогранные аспекты цифровой инклюзии раскрываются на основе информационного подхода к законодательству, который приводит в том числе к необходимости поиска имеющихся рекомендаций, направленных на заполнение указанного пробела и способствующих созданию более инклюзивной и ответственной правовой, общественной и технологической среды.

✉ Контактное лицо

Результаты: исследование темы привело к выводу о необходимости переоценки существующих правовых, общественных и технологических парадигм. Эта переоценка должна быть нацелена на выработку более инклюзивной и доброжелательной концепции доступной среды, которая учитывала бы разнообразие человеческого опыта и потребностей, широкий спектр поведенческих и когнитивных особенностей. Создание особых условий на рабочем месте для лиц с явными и скрытыми проблемами со здоровьем для работодателя должно стать неотъемлемой частью его внимания наряду с вопросами повышения эффективности управления.

Научная новизна: неявные (скрытые) проблемы со здоровьем традиционно не изучаются в должной мере, хотя они охватывают целый спектр психических и физических нарушений, которые, как и явные проблемы со здоровьем, различаются по своему происхождению, интенсивности, постоянному или эпизодическому характеру. Данное исследование восполняет пробел в части поиска ответов на вопросы об инвалидности и ее правовой защите с учетом тренда цифровой инклюзивности, динамического характера современной трудовой деятельности и широкого спектра способностей и потребностей людей.

Практическая значимость: рассматриваемые в исследовании аспекты скрытой или латентной инвалидности позволяют взглянуть на проблему занятости с иной точки зрения, обращая особое внимание на условия, которые можно было бы создать на рабочих местах. Работодатели чаще всего могут не осознавать необходимости создания особых условий труда лицам со скрытыми проблемами со здоровьем, в результате чего увеличивается безработица, растет число больничных; ограничиваются возможности на рабочем месте и многое другое. Сотрудники часто не стремятся по своему желанию раскрывать работодателям информацию о своих неочевидных проблемах со здоровьем, поэтому работодатели должны содействовать раскрытию такой информации, создавая необходимые условия для этого. Такой подход будет способствовать правовой защите данной категории работников и дальнейшему развитию существующего законодательного регулирования, которое не вполне отвечает современным потребностям и изменившейся реальности.

Для цитирования

Хатсон, Дж., Хатсон, П. (2023). Цифровая инклюзия для людей с расстройствами аутистического спектра: пересмотр существующих правовых моделей и доктринальных концепций. *Journal of Digital Technologies and Law*, *1*(4), 851–879. https://doi.org/10.21202/jdtl.2023.37

Содержание

Введение

Скрытые проблемы со здоровьем охватывают целый спектр психических и физических нарушений, которые, как и явные проблемы со здоровьем, различаются по своему происхождению, интенсивности, постоянному или эпизодическому характеру. При рассмотрении инвалидности на рабочем месте выдвигается аргумент, что обсуждение не затрагивает лиц с одним из самых часто скрываемых нарушений – аутизмом, а также соответствующие правовые обязательства (Neely & Hunter, 2014). Как показали международные исследования канадских ученых, скрытые нарушения могут присутствовать у 40 % лиц, имеющих проблемы со здоровьем (Matthews & Harrington, 2000). Более того, требует внимания статус лица со скрытыми нарушениями, так как он является спорным между здоровым состоянием и наличием диагноза, при этом последствия этой неопределенности затрагивают сферы индивидуальной жизнедеятельности, культурных взглядов, общественной политики и профессиональных практик. По наблюдению Reeve & Gottselig (2011), «поскольку незаметные физические недостатки традиционно не изучались в той же мере, что другие формы инвалидности, работодатели могут не осознавать необходимости создавать особые условия лицам со скрытыми проблемами со здоровьем. Результатом становится безработица, рост числа больничных, ограничение возможностей на рабочем месте и многое другое». Скрытая, или латентная инвалидность – это аспект, позволяющий взглянуть на проблему занятости с иной точки зрения, обращая особое внимание на условия, которые можно было бы создать на рабочих местах.

Более того, в научной литературе, посвященной проблемам занятости и инвалидности, можно отметить вопиющее отсутствие такой темы, как решение работника раскрыть работодателю информацию о своих неочевидных проблемах со здоровьем. Такое раскрытие потенциально выгодно сотруднику, так как может улучшить условия на его рабочем месте, однако оно чревато рисками, т. е. несет в себе как плюсы, так и минусы. Итоговый сценарий представляет собой дилемму для сотрудника с незаметными физическими недостатками (Prince, 2017). Таким образом, именно работодатель должен создать на рабочем месте обстановку, способствующую раскрытию информации о проблемах со здоровьем. Этого можно достичь следующими путями: четко обозначить компетенции, необходимые для выполнения работы; заранее дать полную информацию о доступных способах такого раскрытия; обеспечить возможности для такого раскрытия на всех этапах отбора и приема на работу. Создание особых условий на рабочем месте для лиц с явными и скрытыми проблемами со здоровьем – это скорее исключение, чем правило. Чаще внимание уделяется эффективности управления, прозрачности коммуникаций и инклюзивным практикам. Этот подход соответствует нормам правовой защиты данной категории работников (Patton, 2022).

Следует отметить, что при обсуждении проблемы скрытой инвалидности часто упускают из виду такую категорию, как лица с состояниями аутистического спектра (далее – САС). Ряд заболеваний пользуется вниманием со стороны законодателей и общества, но сложные и разносторонние потребности лиц с САС часто игнорируются. Аутизм по самой своей природе не поддается обобщению, охватывая широкий спектр поведенческих и когнитивных черт, которые могут значительно различаться у разных людей. Неявные и часто неверно понимаемые проявления САС могут привести к ошибкам и недостатку индивидуальной поддержки как на рабочем месте,

так и в более широких социальных контекстах. Как показала практика, существующие законодательные нормы, например Закон об американских гражданах с проблемами со здоровьем (Americans with Disabilities Act, ADA), не вполне отвечают этим специфическим и многогранным потребностям. Невозможность адекватно оценить проблемы и помочь лицам с САС является показателем более широкой системной ошибки, когда правовые, общественные и технологические парадигмы не способны в полной мере описать и отразить весь спектр нейроотличных вариантов. Таким образом, возникает настоятельная необходимость расширить традиционные взгляды на проблему доступности среды, создать по-настоящему инклюзивные условия, отвечающие сложным аспектам реальности, связанным с САС.

В данной статье предпринята попытка как оспорить, так и обогатить современные взгляды относительно доступности среды. Авторы показывают, что так называемые особые потребности, или потребности инвалидов, являются на самом деле общечеловеческими. Признавая значительный прогресс, достигнутый благодаря Закону об американских гражданах с проблемами со здоровьем (ADA), который установил нормы физической доступности и условия для инвалидов по зрению, данное исследование подчеркивает вопиющую недостаточность усилий по удовлетворению разносторонних потребностей нейроотличных лиц. Это относится и к таким состояниям, как дислексия и цветовая слепота. Современная тенденция рассматривать такие потребности как особые вызывает тревогу в данном контексте, поскольку может привести к ненамеренной маргинализации и снижению статуса таких лиц. Кроме того, в работе предпринята попытка критически рассмотреть практику найма специалистов по доступной среде в области технологий и пользовательского интерфейса. Было обнаружено, что современные стратегии рекрутинга зачастую сужены до выполнения специфических требований, таких как потребности слабовидящих; при этом игнорируется более широкий спектр условий для нейроотличных лиц, касающийся обработки информации и когнитивных перегрузок. Этот пробел указывает на прискорбное несоответствие между существующим правовым статусом и сложными жизненными ситуациями нейроотличных лиц. Тщательное исследование проблемы привело к выводу о необходимости переоценки существующих правовых, общественных и технологических парадигм. Эта переоценка должна быть нацелена на выработку более инклюзивной и доброжелательной концепции доступности среды, которая не ограничивалась бы только дизайнерскими решениями, но учитывала широкое разнообразие человеческого опыта и потребностей.

1. Незаметные физические недостатки

Научные работы в области инвалидности и ее правовой защиты фокусируются в основном на проблеме физических недостатков. К примеру, под эпизодической инвалидностью понимается длительное состояние здоровья, существенно влияющее на способность лица участвовать в трудовой деятельности и других сферах общественной жизни. В исследовании канадских ученых McKee et al. (2006) эпизодическая инвалидность характеризуется как «серьезное психическое или физическое состояние, отличающееся колебаниями здоровья и нарушений в различные периоды. Эти периоды и степени нарушений здоровья часто непредсказуемы в отношении тяжести, длительности и возможности разрешения» (с. 35). Раскрывая далее природу эпизодической инвалидности, авторы пишут, что она «может быть постоянной

или временной, угрожающей жизни или хронической, прогрессирующей или стабильной. Эпизодичность определяется наличием повторяющихся, иногда циклически, но обычно непредсказуемо периодов улучшения и ухудшения здоровья» (с. 45). В исследовании утверждается, что по сравнению с другими формами инвалидности лица с эпизодической инвалидностью находятся в особенно ущемленном положении, поскольку эту проблему долгое время не признавали, замалчивали и не пытались решить в рамках программ и мер по работе с инвалидами (с. 34). Организации, работающие с эпизодической инвалидностью, имеют дело с лицами, страдающими от различных болезней, среди которых артрит, некоторые формы рака, болезнь Крона, диабет, гепатит С, ВИЧ/СПИД, психические заболевания, аффективные расстройства, рассеянный склероз.

Напротив, разграничение между явной и скрытой инвалидностью лежит в области проявлений нарушения. Лицо с явной инвалидностью демонстрирует признаки нарушений, видимые окружающим, тогда как скрытая инвалидность остается невидимой, не проявляется в виде физических характеристик или поведенческих особенностей. Поскольку такие нарушения остаются относительно незаметными, они не служат для окружающих сигналом, не обрисовывают ситуацию и не формируют первоначальных ожиданий в ходе социальных контактов. Состояние здоровья или нездоровья не приводит к очевидным изменениям во внешности или поступках человека, в результате чего его инвалидность остается незамеченной и неопознанной при социальном взаимодействии. Такая постановка вопроса подразумевает, что дискриминационные или стереотипные реакции по отношению к этому человеку не возникнут (Prince, 2017).

Однако скрытая инвалидность не относится к какой-либо определенной клинической или социальной категории. Некоторыми учеными предложено рассматривать явную и скрытую инвалидность в ряду различных состояний здоровья и конкретных контекстов. Так, Mollow (2010) обращает внимание на «невозможность абсолютного разграничения между явной и скрытой инвалидностью» (с. 502) и подчеркивает, что данная дихотомия приводит к дополнительным сложностям. Состояние, незаметное стороннему наблюдателю в контексте социальной ситуации, может быть очевидным для работников здравоохранения при диагностическом осмотре. Среди примеров скрытой инвалидности Mollow перечисляет «психические заболевания; некоторые когнитивные нарушения; такие физические состояния, как синдром хронической усталости, хроническая травма от повторяющегося напряжения, непереносимость окружающей среды, фибромиалгия, которые не порождают объективно наблюдаемых телесных изменений» (с. 502). Кроме того, существуют определенные половые различия в отношении восприятия или сокрытия нарушений. Например, Krogh и Johnson (2006) утверждают, что женщины с инвалидностью сильнее подвержены появлению скрытых нарушений, таких как хроническая усталость, чем мужчины. Подобный многогранный взгляд на скрытую инвалидность дает возможность определить нюансы проявления и восприятия нарушений в различных контекстах и разными категориями населения.

Для целей нашего исследования необходимо отметить, что состояния аутистического спектра (ранее известные как расстройства аутистического спектра, РАС) охватывают ряд скрытых нарушений, в том чисел СДВГ, дислексию, дисграфию и дискалькулию (Hodges et al., 2020). Исследования показывают, что данный диагноз стигматизируется, из-за чего работники скрывают его (Hurley-Hanson et al., 2020).

Кроме того, лица с САС могут испытывать комплекс разнообразных симптомов, что требует внимания к различным когнитивным и речевым проблемам. Так, значительная доля лиц с САС испытывает сложности с пониманием речи. Это может проявиться в неспособности воспринимать сложные понятия, метафоры, абстрактные высказывания либо определенные идиоматические выражения, сленг (Smith & White, 2020). Парадоксально, что некоторые лица могут демонстрировать экстраординарные способности в определенных когнитивных сферах, например, запоминании цифровых данных, но при этом испытывать трудности в таких базовых областях, как социальные навыки или эмоциональное восприятие (McCauley et al., 2020). Дихотомия между высоким и низким развитием этих когнитивных функций наглядно показывает неоднозначность и сложность данных нарушений в контексте САС.

Кроме того, феномен низкой переносимости когнитивных перегрузок является критическим аспектом умственных нарушений. Лица, испытывающие когнитивные перегрузки, могут реагировать фрустрацией или стрессом на сложные ситуации или чрезмерное количество стимулов (Higgins et al., 2021). Для них первостепенную важность имеют простота и определенность окружения; при наличии множества альтернатив или сложности выбора они могут оказаться неспособными к действию или испытывать длительное эмоциональное расстройство (Hutson & Hutson, 2023). Что касается речевых нарушений, трудности вызывает широкий спектр таких состояний. Так, заикание, т. е. непроизвольное повторение, растяжение или блокирование звуков речи, влияет на беглость речи (Kharismadewi et al., 2023). Аналогичным образом «захлебывающаяся речь», иногда классифицируемая как нарушение речи, представляет собой быструю, ритмически непоследовательную и синтаксически неорганизованную речь с нарушением беглости (Maruthy & Kelkar, 2023). Другими такими состояниями являются апраксия – моторное нарушение речи, состоящее в трудности формирования звуков речи, и дизартрия – состояние вследствие повреждения мозга, приводящее к невнятной или замедленной речи. Эти примеры показывают многогранность проблем с речью при САС (Shriberg et al., 2019).

Нарушения артикуляции, фонематические и неголосовые нарушения дополнительно усложняют ситуацию. Нарушения артикуляции относятся к физическому порождению звуков речи и включают пропуски, добавления, замены или искажения звуков (Griffen et al., 2022). Фонематические нарушения, напротив, относятся к трудностям различения звуков речи, влияя на понимание и коммуникацию. Неголосовые нарушения состоят в полной неспособности порождать речь. Таким образом, скрытые проблемы сотрудников с САС могут быть глубокими и разнообразными (van Rensburg et al., 2020).

В целом данные наблюдения показывают сложность и многогранность проблемы скрытых нарушений как в когнитивной, так и в речевой сфере в контексте САС. Признание и понимание этих трудностей приводит к необходимости тщательно продумывать меры поддержки людей с САС как в частной, так и в профессиональной жизни, обращая внимание на эмпатию, создание соответствующих условий и признание общечеловеческого характера этих так называемых особых потребностей.

2. Правовая защита

Закон об американских гражданах с проблемами со здоровьем (The Americans with Disabilities Act, ADA) показал свою эффективность в установлении стандартов строительства и оснащения доступной среды для лиц с физическими нарушениями (Morgan, 2021). Однако его положения не затрагивают особые потребности лиц с психическими, эмоциональными нарушениями и умственной отсталостью, включая лиц с состояниями аутистического спектра. Правовая защита инвалидов – это обширная область, объединяющая сферу гражданских прав, законодательство по госзакупкам, производственные правовые нормы и различные уровни административного законодательства как внутри страны, так и на международном уровне. Эта защита направлена на обеспечение доступности, равенства и отсутствия дискриминации в различных сферах, однако она зачастую не охватывает категории населения, о которых мы говорим в данной статье (Hawkins, 2023).

Основой указанной правовой защиты служит гражданское законодательство, которое постулирует равные права для лиц с инвалидностью. Эти законы обычно запрещают дискриминацию в различных контекстах, таких как занятость, доступ в здания, доступ к госуслугам, получение услуг в заведениях общественного питания, магазинах, местах развлечений. Примечательно, что ADA представляет собой пример гражданского законодательства, направленного на устранение дискриминации инвалидов, но устанавливающего технические стандарты для одних случаев и игнорирующего другие (Murphy, 2020).

Законодательство по госзакупкам представляет собой другую важную категорию, направленную на обеспечение доступности при приобретении товаров или услуг. Согласно его положениям, должны выполняться стандарты доступности, особенно государственными организациями. Например, Раздел 508 Закона США о реабилитации и Европейский Стандарт 301 549 Евросоюза устанавливают, что закупке подлежат только продукты, отвечающие критериям доступности. Эти законы оказывают существенное влияние на решения по закупкам как в государственном, так и в частном секторе (Bosio et al., 2022).

Законодательство в сфере производства вводит следующий уровень сложности в зависимости от конкретных отраслей, в которых считается необходимым соблюсти условие доступности. Так, в США принят Закон о доступности средств связи и видео (the 21st Century Communications and Video Accessibility Act, CVAA), посвященный телекоммуникации, а также Закон о доступности авиаперевозок (the Air Carrier Access Act, ACAA), регулирующий пассажирские авиаперелеты (Burks, 2013). Эти законы основаны на признании того факта, что в отдельных отраслях может возникнуть необходимость в конкретных, тщательно продуманных правовых нормах, обеспечивающих доступность среды.

На стыке федерального, местного и международного законодательства возникает комплексная инфраструктура, обеспечивающая доступность веб-сайтов и информационно-коммуникационных технологий (Nath & Liu, 2017). Закон об американских гражданах с проблемами со здоровьем устанавливает обязательную доступность различных цифровых платформ и пользовательских сервисов, включая продажи, развлечения и образование. Закон о доступности средств связи и видео расширяет этот список, охватывая продукты, услуги и устройства для связи (Brooks, 2017). Раздел 508 Закона США о реабилитации, как и соответствующие законы штатов,

устанавливает обязательность закупок наиболее доступных технологий в государственном секторе (Olalere & Lazar, 2011). Отдельные законы штатов, например, Закон об инвалидах и Закон Унру штата Калифорния, также регулируют эту сферу, как и подобные законы, принятые в Корее, Канаде, Великобритании, Австралии (Schoen, 2022). Европейский Закон о доступности среды, пока существующий лишь в форме проекта, обещает ряд положений в сфере продуктов, услуг и устройств в Евросоюзе.

Кроме того, следует различать сущность Закона об американских гражданах с проблемами со здоровьем и Раздела 508 Закона США о реабилитации. Изучение этих законодательных актов прольет свет на их уникальные характеристики и вклад в области прав инвалидов (Taylor & Bicak, 2021). Первый из них представляет собой многогранный акт гражданского права, направленный на ликвидацию дискриминации против лиц с инвалидностью в различных сферах общественной жизни в США (Schall, 1998). Закон подразделяется на пять основных секций, каждая из которых посвящена отдельной сфере.

Раздел I – занятость. В данном разделе подчеркивается запрет на дискриминацию во всех аспектах занятости, включая наем, увольнение, продвижение по службе, компенсации и обучение.

Раздел II – госуслуги, администрация штата, местная администрация. Данный раздел посвящен недопущению дискриминации во всех программах, услугах и мероприятиях, организуемых государственными учреждениями.

Раздел III – места общественного пользования и услуги, оказываемые частными организациями. Этот раздел регулирует частные организации, предоставляющие места общественного пользования, включая широкий спектр заведений, таких как отели, рестораны, кинотеатры.

Раздел IV – телекоммуникации. В данном разделе регулируется предоставление услуг, обеспечивающих телефонную связь для лиц с нарушениями слуха и речи, включая положения о скрытых субтитрах.

Раздел V – разное. Этот раздел охватывает различные аспекты, связанные с ADA, включая взаимосвязи этого закона с другими актами, положениями о государственном иммунитете, о незаконном обороте наркотиков и об оплате адвокатов.

Напротив, Раздел 508 Закона США о реабилитации является отдельным федеральным законом, который устанавливает обязательность доступности электронных и информационных технологий, используемых федеральным правительством. Сюда входят веб-сайты, программное обеспечение, аппаратные средства, электронные документы и др. (Jaeger, 2008). Этот акт стал охватывать вопросы сетевой доступности в январе 2017 г., когда в него были включены уровни A и AA Рекомендаций по доступности сетевого контента (Web Content Accessibility Guidelines, WCAG), заменившие модифицированные положения WCAG 1.0 (Caldwell et al., 2008). Европейское законодательство схоже, например, Европейский Стандарт 301 549 схож с Разделом 508, так как посвящен требованиям доступности госзакупок продуктов и услуг в сфере информационно-коммуникационных технологий (Kous et al., 2021).

Важнейшие различия между ADA и Разделом 508 легко понять, изучив четыре аспекта. В технологическом аспекте ADA не охватывает широкий спектр современных цифровых технологий, тогда как Раздел 508 содержит конкретные положения относительно доступности в этой сфере. Содержание ADA значительно шире, закон охватывает все сферы общественной жизни; напротив, Раздел 508 сосредоточен исключительно на федеральных электронных и информационных технологиях.

Что касается применимости, ADA относится к более широкому спектру лиц, таких как работодатели, государственные органы и бизнес, тогда как применимость Раздела 508 ограничивается в основном федеральными агентствами и организациями, получающими федеральное финансирование или контракты. Наконец, механизмы правоприменения для этих двух законов совершенно различны: согласно ADA, каждый человек, считающий, что он столкнулся с дискриминацией, может подать в суд, тогда как, согласно Разделу 508, претензии следует улаживать с федеральными департаментами или агентствами, ответственными за несоблюдение требований к электронным технологиям или информации.

Сравнение двух законодательных актов позволяет определить круг правовых проблем, с которыми могут столкнуться лица с САС на рабочем месте. Критические различия между этими законами выявляются во всех четырех разделах, что имеет значительные последствия для сотрудников с аутизмом и защиты их прав. Что касается технологического аспекта, отсутствие в ADA всеобъемлющих положений относительно современных цифровых технологий создает пробел в области защиты и поддержки лиц с САС, поскольку им могут потребоваться особые технологические решения. Напротив, положения Раздела 508 о доступности цифровой среды в некоторой степени отвечают этим потребностям; однако этот акт направлен исключительно на федеральные сферы применения электронных и информационных технологий, что ограничивает его значимость.

Что касается содержания, ADA отличается более широким охватом общественной жизни, т. е. теоретически этот закон должен давать более существенную защиту работникам с САС. Напротив, Раздел 508 имеет более узкую направленность, оставляя незащищенными особые потребности таких лиц, если они не работают в федеральных агентствах. В отношении применимости Закон ADA также охватывает работодателей, государственные органы и бизнес, т. е. должен затрагивать более широкий круг лиц с САС. Раздел 508, касающийся только федеральных агентств и организации с федеральным финансированием и контрактами, исключает из сферы своего действия значительную долю трудовых ресурсов, что дополнительно маргинализирует работников с САС в профессиональной области.

Наконец, отдельный круг проблем возникает в связи с различными механизмами правоприменения этих двух законов. Возможность индивидуальных исков против дискриминации согласно ADA позволяет напрямую добиться изменения ситуации. Напротив, процедуры подачи жалоб согласно Разделу 508 более запутанны; иски должны подаваться в адрес отдельных федеральных министерств или агентств, это может создавать барьеры для лиц с САС, столкнувшихся с несоблюдением требований в области электронных и информационных технологий. В совокупности эти различия в законодательстве рисуют сложную и зачастую противоречивую картину законных прав и мер защиты, которые предлагаются лицам с аутизмом. Черты сходства и несоответствия между ADA и Разделом 508 указывают на насущную необходимость прибегнуть к целостному и тщательно продуманному подходу, учитывающему все многогранные потребности лиц с САС на рабочем месте. Такой подход требует полной переоценки существующих правовых норм, а также твердой приверженности принципам инклюзивности и эмпатии в трудовой сфере, которые понимаются шире, чем просто исполнение закона.

3. Практическая поддержка

Ряд исследований посвящены сложностям, возникшим у обсуждаемой категории граждан в связи с пандемией COVID-19. К примеру, в работе Capuano (2022) были изучены глубокие изменения в трудовых процессах, вызванные пандемией, и их последствия для законодателей в Австралии. Выявлена тенденция развития гибридных и совместных рабочих позиций. Исследование показало, что такой сдвиг парадигмы несет в себе риски неравенства и косвенной дискриминации для лиц со скрытой инвалидностью. Автор утверждает, что такой режим работы ставит в невыгодное положение сотрудников со скрытыми физическими недостатками, тем самым порождая новый уровень трудового неравенства. Анализ трудового и антидискриминационного законодательства Австралии показал, что современные правовые структуры не в состоянии справиться с этими новыми угрозами. Так, существующие законы не учитывают сложностей, с которыми сталкиваются сотрудники со скрытыми физическими недостатками на рабочем месте после пандемии. Более того, когда такие сотрудники пытаются подать иски согласно Закону о справедливых трудовых отношениях (Fair Work Act) или против косвенной дискриминации согласно существующему законодательству, такие иски часто несправедливо отклоняют. Отмечается, что это происходит не из-за недостаточной обоснованности жалоб, а по причине недостатков в самой правовой системе. Выдвигаются предложения по реформированию как Закона о справедливых трудовых отношениях, так и различных национальных местных антидискриминационных законов, чтобы лица со скрытыми физическими недостатками могли получать равноправную защиту с теми, кто имеет явную инвалидность (Farbenblum & Berg, 2017).

По тем же причинам и в свете растущего количества случаев аутизма возникает необходимость применять более универсальные решения проектировщикам и архитекторам. Так, Clouse et al. (2020) представили методологию проектирования в соответствии с нормами ADA, отвечающего потребностям лиц с САС. С этой целью проектировщики и архитекторы должны знать и учитывать сенсорные трудности, которые испытывают лица с САС при взаимодействии с нейротипичными людьми. Кроме того, особые дизайнерские решения могли бы помочь учителям, врачам и родителям детей с аутизмом выстраивать более успешное взаимодействие. Окружающая среда с избытком стимулов может подорвать все усилия родителей и врачей по достижению соответствующих целей.

Одно из возможных решений предложено в работе Mostafa (2014). Автор выделяет семь принципов проектирования, обозначая их акронимом ASPECTSS: Acoustics (акустика), Spatial sequencing (планирование пространства), Escape spaces (убежища), Compartmentalization (обособление зон), Transition spaces (переходные зоны), Sensory zoning (сенсорное зонирование), Safety (безопасность). Специально разработанные для лиц с САС, эти принципы служат основой для практических решений. Проектировщики и архитекторы должны придерживаться этических принципов создания инклюзивной среды. Авторы приводят в пример проекты центра профессиональной подготовки, в одном из которых соблюдаются требования ADA, а в другом дополнительно представлены свойства, отвечающие потребностям лиц с САС. Указанные принципы были созданы на основе наблюдений, изучения научной литературы и личных собеседований. Они свидетельствуют о том, что продуманный подход к потребностям лиц с САС не только позволяет достичь поставленной цели,

но и улучшает среду для окружающих. Это важное доказательство того, что разработки должны не только выполнять требования закона, но и способствовать инклюзивности и эмпатии.

Законы в отношении создания условий для инвалидов, особенно на рабочем месте, всегда затрагивали аспекты проектирования и архитектуры (Hawkins, 2023; Murphy, 2020). Этот подход определил существующее законодательство, регулирующее рекомендации и требования преимущественно для обеспечения доступности физических объектов, от пандусов и лифтов до туалетов. Эти материальные аспекты стали наглядным проявлением создания условий для инвалидов. Однако этот традиционный подход не учитывает важнейшую часть трудовой деятельности в современном мире – цифровую сферу.

4. Рекомендации

Существенная доля повседневных контактов и профессиональных задач в сегодняшнем мире выполняется на цифровых площадках (Baptista et al., 2020). Такие действия, как печатание на клавиатуре, чтение с экрана, участие в виртуальных собраниях, составляют неотъемлемую часть трудовой деятельности. Следовательно, понятие доступности претерпело фундаментальные изменения, что приводит к необходимости пересмотреть существующие правовые нормы. Таким образом, нынешний акцент на архитектурных приспособлениях уже не отражает всю сложность цифровой среды; теперь доступность может относиться к таким факторам, как удобство чтения с экрана, функциональность клавиатуры, когнитивные требования пользовательских интерфейсов. Для лиц с различными нарушениями, включая нейроотличные состояния, эти цифровые взаимодействия могут стать такими же непреодолимыми барьерами, как и физические препятствия. Однако существующее законодательство по-прежнему отстает в вопросе признания и учета проблем цифровой доступности (Inal et al., 2020).

Разрыв между традиционной правовой точкой зрения на особые условия для инвалидов и насущными потребностями на цифровом рабочем месте ярко показывает пробел в понимании концепции доступности. Без сомнения, архитектурные аспекты не теряют своего значения, но они уже недостаточны при обсуждении особых условий для инвалидов. Переход к цифровой рабочей среде требует комплексного понимания доступности, объединяющего физические аспекты проектирования и многогранные аспекты цифровой инклюзии (de Melo et al., 2022). Такое понимание невозможно без проактивного и информированного подхода к законодательству, которое отвечает динамическому характеру современной трудовой деятельности и широкому спектру способностей и потребностей людей. Оно также приводит к необходимости изучить имеющиеся рекомендации, направленные на заполнение указанного пробела и способствующие созданию более инклюзивной и ответственной правовой, общественной и технологической среды.

В более ранних исследованиях были описаны стратегии развития нейроинклюзивности на рабочих местах. Обеспечение условий для нейроотличных сотрудников требует значительных изменений существующих практик. Рекомендации для таких изменений основаны на принципе индивидуализированного, персонифицированного общения. Руководство и коллеги должны давать ясные, четкие пошаговые инструкции, минимизируя двусмысленность и облегчая понимание. Благоприятная

и предсказуемая среда создается также путем учета особенностей работы и общения, например, установления точных сроков выполнения работ и заблаговременных оповещений о собраниях. Необходимы определенные и четкие инструкции без абстрактных и двусмысленных формулировок, визуальные сигналы для напоминания о важных аспектах, сообщения о повестке собраний. Особенности социального взаимодействия нейроотличных лиц требуют сократить незначащее общение, предлагать способы выхода из общения, позволить не использовать камеру на видеоконференциях. В целом эти рекомендации объединены подходом, для которого характерно признание особых потребностей и предпочтений нейроотличных сотрудников. Этот подход не только способствует эффективной коммуникации и сотрудничеству, но и отражает глубокое уважение к нейроотличным лицам, тем самым превосходя традиционные нормы и создавая более инклюзивную, эмпатичную и продуктивную среду на рабочем месте (Hutson & Hutson, 2023).

Если существующие рекомендации фокусируются на свойствах среды, то в наши дни в центре внимания должны оказаться условия цифровой доступности, учитывая характер труда в цифровую эпоху. В то же время комплексный подход с целью достижения цифровой инклюзивности требует реализации пяти отдельных тематических аспектов: восприятия, функциональности, понятности, целостности и особых технических мер. Каждый из этих аспектов играет важнейшую роль в обеспечении взаимодействия нейроотличного индивида с цифровой средой.

Восприятие в контексте цифрового дизайна для нейроотличных лиц представляет собой разностороннюю деятельность. Конечной целью улучшения восприятия является доступность цифрового контента в различных формах, отвечающих разнообразным потребностям в восприятии. Одним из примеров служит предоставление текстовой альтернативы для нетекстового контента. Например, субтитры к видеозаписи позволяют получать информацию лицам с нарушениями слуха, а текстовые описания изображений помогают незрячим понять видеоконтент через программу для чтения экрана (Kous et al., 2020). Эти варианты можно затем преобразовать в шрифт Брайля, речь, вывести крупным шрифтом, чтобы обеспечить доступность разными способами.

Аналогичным образом развернутые во времени материалы, такие как видео или мультипликация, должны быть дополнены другими методами восприятия, например, подписями или переводом на язык жестов. Хороший пример дают образовательные площадки, предлагающие лекции с субтитрами, что позволяет эффективно воспринимать контент как лицам с нарушениями слуха, так и носителям других языков. Кроме того, если контент представлен в различных форматах, его целостному и структурному восприятию помогает правильное расположение материала на странице (Duarte & Fonseca, 2019). Например, использование макета гибкой сетки обеспечивает необходимое положение контента при изменении размера изображения или переходе на мобильное приложение. Такая гибкость как нельзя лучше подходит пользователям, которые увеличивают размер шрифта или применяют цветовые контрасты, не нарушая общей структурной целостности контента (Lister et al., 2020).

Другой важнейший аспект восприятия состоит в разнице между фоном и содержанием, которая влияет как на зрительное, так и на слуховое понимание. Хорошим примером служат веб-сайты, предлагающие «темный режим», так как некоторые пользователи плохо воспринимают яркий фон (Willmore & King, 2023). Кроме того, в мультимедиа могут применяться четко различающиеся аудиоканалы, помогающие лицам со слуховыми трудностями справляться с несколькими источниками звука.

Аспект восприятия затрагивает также проблему использования мультисенсорности. К примеру, тактильный отклик в интерфейсах сенсорных экранов помогает лицам с нарушениями зрения. Гаптика – сенсорная технология, стимулирующая тактильные ощущения, – представляет собой инновационное направление, расширяющее доступность путем задействования различных органов чувств (Michelsanti et al., 2021).

Функциональность в контексте цифрового дизайна означает способность эффективно взаимодействовать с цифровым контентом и осуществлять навигацию по нему. Это понятие охватывает множество компонентов и является важнейшим для обеспечения инклюзивности как нейроотличных индивидов, так и лиц с иными нарушениями. Главное положение функциональности состоит в доступности всех функций через различные средства ввода, не ограниченные только клавиатурой. Это такие альтернативные средства ввода, как голосовые команды, прикосновения, движения глаз (Lowndes & Connelly, 2023). Например, такие программы распознавания речи, как Dragon Naturally Speaking, дают возможность людям с нарушениями подвижности осуществлять навигацию и управлять приложениями с помощью голосовых команд (Vickers et al., 2022). Также адаптивные технологии, такие как отслеживание движений глаз, позволяют лицам с ограничениями моторных функций взаимодействовать с цифровым контентом.

Важно дать пользователям достаточно времени для восприятия и взаимодействия с контентом. Предположим, на веб-сайте банка используется ограничение времени с целью безопасности; в таком случае нужно дать пользователям возможность запросить дополнительное время, чтобы те, кому требуется больше времени для навигации, не оказались выброшены с сайта. Кроме того, ценной функцией является изменение скорости видео, что позволяет воспринимать информацию в комфортном режиме (Seo et al., 2021). При этом краеугольным камнем функциональности является эффективная навигация. Необходимо делать ее более интуитивной с помощью таких инструментов, как навигационные цепочки, ясные заголовки, последовательные меню, описательные ссылки. К примеру, использование ссылок вида «перейти к содержанию» позволяет пропустить повторяющиеся элементы навигации и быстрее достичь основного контента (Pham et al., 2023).

Пристальное внимание должно быть уделено элементам дизайна, которые могут вызвать приступ эпилепсии. Живым напоминанием о рисках при быстрой смене видеоизображений или определенных цветовых сочетаний служит инцидент с покемоном, вызвавшим судорожные припадки у 685 детей, как указано в Руководстве по предотвращению приступов эпилепсии (Seizure Prevention Guidelines, 1997). Современные руководства по веб-дизайну подчеркивают необходимость придерживаться безопасных цветовых сочетаний и ограничивать частоту визуальных вспышек, чтобы избежать таких рисков для здоровья. Таким образом, внимание к индивидуальным предпочтениям пользователя показывает всю сложность проблемы функциональности (Ferlazzo et al., 2021). Настраиваемый размер шрифта, цветовые схемы, форматы позволяют пользователям приспособить интерфейс к своим нуждам. К примеру, такие площадки, как My Web, My Way компании BBC[1], позволяют пользователям задать размер и цвет шрифта, другие свойства изображения, чтобы повысить читабельность и комфорт. В целом функциональность в контексте цифрового

[1] https://goo.su/ynhV7

дизайна – это нечто большее, чем просто функциональность; она воплощает пользовательско ориентированный подход, сутью которого являются признание и учет различных потребностей и предпочтений всех пользователей (Proença et al., 2021).

Понятность в контексте цифрового дизайна означает легкость, с которой пользователи могут интерпретировать, понимать и взаимодействовать с контентом. Для лиц с когнитивными нарушениями, включая САС, факторы, влияющие на понятность, могут значительно менять способность действовать в цифровой среде. В работе (Zubala et al., 2021) перечислены различные аспекты понятности и даны примеры, раскрывающие ее значимость. Так, понятность текста зависит от его читабельности, факторы которой включают размер и вид шрифта, длину строк, цветовой контраст. Веб-сайты, использующие специальные шрифты для дислексиков и большой межстрочный интервал, могут существенно повысить свою привлекательность для этой категории читателей. Кроме того, применяется контрастность согласно Рекомендациям о доступности сетевого контента (Web Content Accessibility Guidelines, WCAG), которую можно проверить с помощью специальных инструментов, таких как accessible; речь идет о разнице между понятным и полностью нечитаемым текстом для лиц со зрительными нарушениями (Panda & Chakravarty, 2020).

Навигацию и понимание текста облегчают использование семантических заголовков и соблюдение логической структуры. Правильно размещенные заголовки (например, после заголовка 1 следуют заголовки 2 и 3) не только создают визуальную иерархию, но и позволяют судить о структуре содержания текста, тем самым облегчая навигацию пользователям с нарушениями зрения. Кроме того, четкое разделение на секции и последовательное оформление дают возможность читателю предсказать, где находится интересующая его информация, что снижает умственную нагрузку (Fayyaz & Khusro, 2023). Аналогичным образом доступное полнофункциональное интернет-приложение (Accessible Rich Internet Applications, ARIA) использует символы в рамках технологии специальных возможностей, которые обозначают отдельные области сетевого контента, такие как баннеры, главная страница, области навигации, область поиска. Например, если определенная область обозначена как «главная страница», то пользователь может перейти сразу на нее, минуя промежуточные ссылки. Такая направленная навигация повышает эффективность работы и понимание пользователей в рамках технологии специальных возможностей (Blanco et al., 2022).

Понятность можно повысить с помощью ясных инструкций, которые позволяют пользователям предотвратить или исправить свои ошибки. К примеру, на сайте электронной торговли можно организовать проверку заполнения форм в реальном времени с подсвечиванием неверно заполненных полей и выводом соответствующих сообщений, например, «Неверный формат адреса электронной почты». Такая немедленная обратная связь дает пользователям возможность понять и исправить ошибки без смущения или подавленности. Предсказуемость в работе веб-страницы минимизирует ощущение путаницы и когнитивной перегрузки. Сюда же относятся наличие последовательных меню во всех разделах сайта, предсказуемые реакции на действия пользователя (такие как нажатие на кнопку), понятные предупреждения о важных изменениях, таких как открытие нового окна или вкладки. Существуют автоматизированные инструменты, например, Keros, которые облегчают выполнение требования понятности через такие технологии, как анализ цветового контраста; они обеспечивают соблюдение общепринятых норм и стандартов, не требуя

специальных знаний в этой области (Teh & Ramli, 2023). Таким образом, понятность как аспект цифрового дизайна включает в себя сложный баланс визуальной эстетики, структуры контента, управления действиями пользователя и технологической поддержки. Используя такие инструменты, как семантические заголовки, символы ARIA, автоматические проверки, дизайнеры и разработчики могут создать цифровую среду, которая будет не только доступной, но и понятной и привлекательной для всех пользователей, включая лиц с когнитивными нарушениями (Blanco et al., 2022).

Целостность в цифровом дизайне подразумевает устойчивость и адаптивность системы при использовании различных платформ и технологий, включая инструменты технологии специальных возможностей. Это свойство выходит за пределы простой функциональности и представляет собой тонкую интеграцию визуальной эстетики и функциональной доступности. Рассмотрим ключевые элементы целостного дизайна и приведем примеры практического применения данных принципов. Для обеспечения целостности необходимо учесть потребности лиц, работающих с клавиатурой одной рукой. Это могут быть временные состояния, например сломанная рука, или постоянные нарушения, препятствующие использованию обеих рук. Для таких категорий пользователей веб-сайты и приложения предлагают ввод команд одной клавишей, пиктограммы ускоренного доступа, навигацию с помощью вкладок. Например, применение режима залипающих клавиш позволяет нажимать клавиши последовательно, а не одновременно, что облегчает работу одной рукой. Этот метод повышения доступности при работе на компьютере привлек большое внимание благодаря возможности помочь людям с физическими недостатками или моторными нарушениями (Thompson & Copeland, 2020).

Использование замещающего текста для изображений обеспечивает доступность контента для лиц, пользующихся программами для чтения экрана, а также при отключении изображений, например, при низкой пропускной способности. Описательный замещающий текст, например, «Группа сотрудников вокруг стола в конференц-зале», дает контекст и информацию, поддерживает разнообразие и смысл контента. Такой подход отвечает принципу целостности, так как позволяет воспринимать визуальный контент различным категориям пользователей. Аналогичным образом использование невидимых ярлыков для элементов форм повышает доступность, не нарушая визуального дизайна. Такие ярлыки визуально скрыты, но передаются программами для чтения экрана, что позволяет пользователям с нарушениями зрения понимать и взаимодействовать с формами. Например, в форме регистрации поля «Имя пользователя» и «Пароль» визуально скрыты, однако считываются с помощью технологии специальных возможностей (Gleason et al., 2020).

Таблицы представляют сложную информацию в легко воспринимаемом формате, но в отсутствие продуманного дизайна она могут стать барьером для пользователей с нарушениями. Используя правильные заголовки и соответствующее расположение строк и столбцов, можно повысить доступность табличного материала. Связи между заголовками и ячейками задаются с помощью таких инструментов в режиме HTML, как «масштаб» (scope). Тем самым информация становится понятной лицам, пользующимся технологией специальных возможностей. Целостность в дизайне предполагает не только применение современных технологий, но и учет будущих достижений. Чтобы контент оставался таким же доступным и целостным спустя время, необходимо использовать стандартные методы кодирования, избегать устаревших приемов, тестировать продукт на различных браузерах и устройствах.

Кроме того, стандарты доступности обеспечиваются выполнением требований таких современных норм, как Рекомендации о доступности сетевого контента (WCAG) (Zhang & Balog, 2020).

Целостность – это не только технические спецификации, но и своего рода сплав эстетики и функциональности. Безупречное слияние визуального дизайна и учета потребностей пользователей отражает комплексный подход к принципу доступности, в котором объединяются и различные приемы, и предпочтения пользователей, и технологические условия. Применяя такие стратегии, как возможность работы одной рукой, замещающий текст, скрытые ярлыки, стандартные методы кодирования, дизайнеры и разработчики могут создавать надежную и адаптивную цифровую среду. Целостность дизайна не только обеспечивает соблюдение правовых норм, но и отвечает этическим требованиям, подчеркивая достоинство и личностное многообразие всех пользователей.

Особые технические меры – это последняя область повышения цифровой инклюзивности, включающая в себя разнообразные специализированные методы, позволяющие усилить доступность среды. Эта область представляет собой синтез компонентов, требующих большого внимания к деталям. В том, что касается доступности, сложные решения должны отвечать индивидуальным потребностям. При этом, чтобы обрисовать эту сложную область, необходимо детально изучить особые технические меры, в том числе на практике. Прежде всего, это комплекс доступных полнофункциональных интернет-приложений (ARIA), позволяющих сделать сетевой контент доступным для людей с инвалидностью. Атрибуты роли, состояния и свойств ARIA могут быть добавлены в HTML, тем самым повышая доступность виджетов JavaScript, таких как бегунки, меню, диалоговые окна (Chiou et al., 2021). К примеру, интегрируя такие роли ARIA, как «бегунок» или «кнопка», разработчики могут обеспечить корректную совместимость между этими виджетами и технологиями специальных возможностей при использовании программ для чтения экрана.

Другой необходимой мерой является обеспечение цветового контраста между текстом и фоном, что очень важно для лиц с нарушениями зрения, включая цветовую слепоту. Такие инструменты, как WebAIMcolor, позволяют проверить и установить нужные значения контраста в соответствии с Рекомендациями WCAG. Например, соотношение контрастности текста к фону 4,5 : 1 существенно облегчает чтение людям со слабым зрением (Frey & Mancilla, 2023). То же касается социальных сетей, которые стали неотъемлемой частью современной коммуникации, а значит, доступность этих платформ жизненно важна. Работа программ для чтения экрана значительно улучшается при использовании таких мер, как описания изображений в «Твиттере[2]» или использование «верблюжьего регистра» (слитного написания слов с заглавными буквами) в хештегах (например, #ЦифроваяДоступность) (Kausar et al., 2021). Такие приемы позволяют лицам со зрительными или когнитивными нарушениями полноценно взаимодействовать с контентом социальных сетей.

Этот подход предполагает усиление синтаксиса HTML атрибутами WAI-ARIA для получения дополнительной информации о доступности. Совместимость между технологиями специальных возможностей обеспечивается за счет использования

[2] Социальная сеть, заблокированная на территории Российской Федерации за распространение незаконной информации.

ролей, состояний и свойств, определяющих отношения доступности между элементами среды. Применение особых технических мер для обеспечения цифровой доступности требует детального понимания и точного выполнения различных стратегий (табл. 1). Каждый элемент, от интеграции ARIA до доступности социальных сетей, играет жизненно важную роль в построении инклюзивного цифрового опыта (Žuliček et al., 2021). Применяя эти подходы, дизайнеры и разработчики могут сконструировать сетевой контент таким образом, чтобы он отвечал не только правовым стандартам, но и всему многообразию потребностей пользователей.

Таблица 1. Факторы повышения цифровой доступности для нейроотличных лиц

Фактор	Рекомендации по повышению цифровой доступности
Восприятие	– Предоставить текстовые альтернативы для нетекстового контента (например, письменность по Брайлю, речь). – Предложить альтернативы для материалов, развернутых во времени. – Расположить контент так, чтобы позволить различное представление без потери информации. – Усилить разграничение фона и содержания для лучшего визуального и слухового восприятия
Функциональность	– Обеспечить доступность всех функций через различные средства ввода (клавиатуру, касание, голос и др.). – Дать пользователям достаточно времени для восприятия контента. – Устранить элементы дизайна, которые могут вызвать припадок. – Облегчить навигацию и поиск контента
Понятность	– Обеспечить читабельность текста и предсказуемость содержания веб-страниц. – Использовать семантические заголовки и символы ARIA. – Использовать такие инструменты, как Keros, для анализа цветового контраста
Целостность	– Улучшить взаимодействие с помощью таких технологий, как работа с клавиатурой одной рукой. – Использовать замещающий текст для изображений и невидимые ярлыки для элементов форм. – Обеспечить совместимость с современными и будущими агентами пользователя, включая технологии специальных возможностей. – Использовать заголовки таблиц и другие элементы дизайна, не изменяющие визуальный дизайн
Особые технические меры	– Интегрировать символы ARIA для виджетов на JavaScript. – Выполнять требования цветового контраста, например, с помощью программы WebAIM Color Contrast Checker. – Повышать доступность социальных сетей, включая описания изображений и «верблюжий регистр» (слитное написание слов с заглавными буквами) в хештегах. – Делать ссылки для быстрого перехода в навигации. – Учитывать когнитивные нарушения при разработке дизайна. – Интегрировать символы WAI-ARIA в синтаксис HTML для совместимости с технологиями специальных возможностей

В попытке создать инклюзивную и доступную цифровую среду для нейроотличных лиц всемерный учет пяти важнейших факторов: восприятия, функциональности, понятности, целостности и особых технических мер – составляет структурированный подход к удовлетворению разнообразных потребностей. Рекомендации, выработанные в этой сфере, отражают множество аспектов, которые следует учесть для обеспечения полной инклюзии для всех пользователей, независимо от их нейроотличного

статуса. Такой многогранный подход соответствует более широкому пониманию инклюзивности и равенства в виртуальном мире. Сплав визуальной эстетики, функциональной доступности, скрупулезного внимания к деталям воплощает в себе универсальный пользовательский опыт, который не ограничивается лишь следованием существующим стандартам. Строгая приверженность этим принципам, выявленным с помощью конкретных примеров и экспертных оценок, задает основу, чтобы дизайнеры, разработчики и законодатели могли построить будущее, в котором социальные ценности инклюзивности и эмпатии найдут свое продолжение в цифровой среде. Будущее цифрового дизайна лежит в области признания и учета неотъемлемого разнообразия человеческого опыта, а четкие рекомендации освещают направление движения к этому будущему.

Заключение

Представленный анализ выявил необходимость обратить существенное внимание на проблему скрытой инвалидности на рабочем месте, особенно при состояниях аутистического спектра. Таким образом, мы критически рассмотрели как существующую ограниченность Закона об американских гражданах с проблемами со здоровьем, так и детальные рекомендации в рамках соответствующего раздела. Поднятая в исследовании проблема сложна и многогранна, поэтому требует дальнейшей разработки.

Скрытая инвалидность на рабочем месте – это комплексное явление, которое часто остается непризнанным. Указанные состояния, включая САС, не всегда очевидны, однако они могут значительно влиять на способность человека функционировать на рабочем месте в традиционной среде. Следствия из этого затрагивают более широкую область инклюзивности, поскольку возникает вопрос, можно ли создать на рабочем месте среду, удобную для всех сотрудников, даже имеющих какие-либо скрытые нарушения. В отношении САС, особенно нейроотличных лиц, ситуация еще более осложняется, учитывая широкий спектр проявлений и их взаимодействий со средой. Необходимо ценить уникальные сильные стороны и особенности лиц с САС и создавать меры поддержки, учитывающие эти характеристики. Таким образом, следует признать, что условия на рабочем месте должны быть не только приспособленными к их потребностям, но и выстраивать более инклюзивную и универсальную среду.

В этом контексте становится очевидной ограниченность существующего законодательства – Закона об американских гражданах с проблемами со здоровьем. Данный закон был первым в этой области, однако в нем недостаточно учтены особые потребности лиц со скрытыми нарушениями, включая САС. Сосредоточенность этого закона на физической доступности иногда затмевает разнообразные потребности лиц с когнитивными нарушениями и пороками развития, результатом чего становятся пробелы в создании условий или мер поддержки. Заполнить некоторые из этих пробелов призваны рекомендации данной статьи. В них подчеркнута необходимость переоценки существующих правовых норм, всестороннего сотрудничества между работодателями и юристов по делам инвалидов, а также важность коллективной поддержки на уровне сообществ. Однако выполнение этих рекомендаций не лишено трудностей, оно требует взвешенного подхода с учетом сложных взаимосвязей между индивидуальными потребностями, организационной культурой и нормами закона.

Таким образом, необходимы дальнейшие комплексные исследования в русле указанных трудностей и представленных рекомендаций. Они должны состоять в эмпирическом изучении практики создания условий для лиц со скрытыми нарушениями, включая САС, на рабочих местах. Также чрезвычайно актуальны правовые исследования, которые могли бы критически оценить эффективность ADA в контексте скрытой инвалидности и выработать рекомендации для возможных изменений или дополнений. Кроме того, для более детального понимания проблемы было бы целесообразно применить междисциплинарный подход, объединяющий такие области, как психология, социология, организационное поведение и право. Сотрудничество между компаниями, юристами по делам инвалидов и лицами с нарушениями здоровья придало бы глубину и обоснованность такому исследованию.

Список литературы

Baptista, J., Stein, M. K., Klein, S., Watson-Manheim, M. B., & Lee, J. (2020). Digital Work and Organisational Transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, *29*(2), 101618. https://doi.org/10.1016/j.jsis.2020.101618

Blanco, M., Zong, J., & Satyanarayan, A. (2022). *Olli: An Extensible Visualization Library for Screen Reader Accessibility*. https://vis.mit.edu/pubs/olli.pdf

Bosio, E., Djankov, S., Glaeser, E., & Shleifer, A. (2022). Public Procurement in Law and Practice. *American Economic Review*, *112*(4), 1091–1117. https://doi.org/10.1257/aer.20200738

Brooks, A. (2017). Accessibility: Definition, Labeling, and CVAA Impact. *Recent Advances in Technologies for Inclusive Well-Being: From Worn to Off-body Sensing, Virtual Worlds, and Games for Serious Applications*, 283–383. https://doi.org/10.1007/978-3-319-49879-9_14

Burks, C. L. (2013). Improving Access to Commercial Websites Under the Americans with Disabilities Act and the Twenty-First Century Communications and Video Accessibility Act. *Iowa Law Review, 99*(1), 363. https://clck.ru/36kuL4

Caldwell, B., Cooper, M., Reid, L. G., Vanderheiden, G., Chisholm, W., Slatin, J., & White, J. (2008). *Web Content Accessibility Guidelines (WCAG) 2.0. WWW Consortium (W3C)*, *290*, 1–34. https://clck.ru/36kuNe

Capuano, A. (2022). Post-Pandemic Workplace Design and the Plight of Employees with Invisible Disabilities: In Australian Labour Law and Anti-Discrimination Legislation Equipped to Address New and Emerging Workplace Inequalities?. *The University of New South Wales Law Journal*, *45*(2), 873–913. https://doi.org/10.53637/emwr6179

Chiou, P. T., Alotaibi, A. S., & Halfond, W. G. (2021, August). Detecting and Localizing Keyboard Accessibility Failures in Web Applications. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 855–867). https://doi.org/10.1145/3468264.3468581

Clouse, J. R., Wood-Nartker, J., & Rice, F. A. (2020). Designing Beyond the Americans with Disabilities Act (ADA): Creating an Autism-Friendly Vocational Center. *HERD: Health Environments Research & Design Journal*, *13*(3), 215–229. https://doi.org/10.1177/1937586719888502

de Melo, F. D. A. F., Soares, K. P., de Barros, E. M., dos Santos Cabral, E. L., da Costa Júnior, J. F., da Silva, A. A. R. S., & Burlamaqui, A. M. F. (2022). Inclusive Digital Technologies in the Classroom: A Case Study Focused on Students with Autism Spectrum Disorder (ASD) in the Final Years of Elementary School. *Research, Society and Development*, *11*(6), e10211628759-e10211628759. https://doi.org/10.33448/rsd-v11i6.28759

Duarte, C., & Fonseca, M. J. (2019). *Multimedia Accessibility. In Web Accessibility: A Foundation for Research* (pp. 461–475). Springer, London. https://doi.org/10.1007/978-1-4471-7440-0_25

Farbenblum, B., & Berg, L. (2017). Migrant Workers' Access to Remedy for Exploitation in Australia: The Role of the National Fair Work Ombudsman. *Australian Journal of Human Rights*, *23*(3), 310–331. https://doi.org/10.1080/1323238x.2017.1392478

Fayyaz, N., & Khusro, S. (2023). Enhancing Accessibility for the Blind and Visually Impaired: Presenting Semantic Information in PDF Tables. *Journal of King Saud University – Computer and Information Sciences*, 101617. https://doi.org/10.1016/j.jksuci.2023.101617

Ferlazzo, E., Sueri, C., Masnou, P., Aguglia, U., Mercuri, S., Caminiti, E., & Piccioli, M. (2021). Technical Issues for Video Game Developers and Architects to Prevent Photosensitivity. In *The Importance of Photosensitivity for Epilepsy* (pp. 407–412). Springer, Cham. https://doi.org/10.1007/978-3-319-05080-5_33

Frey, B. A., & Mancilla, R. (2023). Inclusive Online Learning: Digital Accessibility Practices. In *Diversity in Higher Education Remote Learning: A Practical Guide* (pp. 93–104). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-31214-4_8

Gleason, C., Pavel, A., McCamey, E., Low, C., Carrington, P., Kitani, K. M., & Bigham, J. P. (2020, April). Twitter A11y: A Browser Extension to Make Twitter Images Accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). https://doi.org/10.1145/3313831.3376728

Griffen, B., Woods-Catterlin, L., Lorah, E. R., & Whitby, P. S. (2022). Teaching Communication to Individuals with Autism Spectrum Disorders. In *Autism Spectrum Disorders: Advancing Positive Practices in Education.* (5th Ed.). Routledge. https://doi.org/10.4324/9781003255147-9

Hawkins, D. S. (2023). Overlooked and Undercounted: Communication and Police Brutality Against People with Disabilities. In *The Palgrave Handbook of Disability and Communication* (pp. 385–399). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-14447-9_23

Higgins, J. M., Arnold, S. R., Weise, J., Pellicano, E., & Trollor, J. N. (2021). Defining Autistic Burnout Through Experts by Lived Experience: Grounded Delphi Method Investigating #AutisticBurnout. *Autism*, *25*(8), 2356–2369. https://doi.org/10.1177/13623613211019858

Hodges, H., Fealko, C., & Soares, N. (2020). Autism Spectrum Disorder: Definition, Epidemiology, Causes, and Clinical Evaluation. *Translational Pediatrics*, *9*(Suppl 1), S55. https://doi.org/10.21037/tp.2019.09.09

Hurley-Hanson, A. E., Giannantonio, C. M., Griffiths, A. J., Hurley-Hanson, A. E., Giannantonio, C. M., & Griffiths, A. J. (2020). The Stigma of Autism. *Autism in the Workplace: Creating Positive Employment and Career Outcomes for Generation A* (pp. 21–45). https://doi.org/10.1007/978-3-030-29049-8_2

Hutson, P., & Hutson, J. (2023). Neurodiversity and Inclusivity in the Workplace: Biopsychosocial Interventions for Promoting Competitive Advantage. *Journal of Organizational Psychology*, *23*(2), 1–16. https://doi.org/10.33423/jop.v23i2.6159

Inal, Y., Guribye, F., Rajanen, D., Rajanen, M., & Rost, M. (2020, October). Perspectives and practices of digital accessibility: A survey of user experience professionals in Nordic countries. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1–11). https://doi.org/10.1145/3419249.3420119

Maruthy, S., & Kelkar, P. (Eds.). (2023). *Understanding and Managing Fluency Disorders: From Theory to Practice.* Routledge. https://doi.org/10.4324/9781003367673

Jaeger, P. T. (2008). User-Centered Policy Evaluations of Section 508 of the Rehabilitation Act: Evaluating E-Government Web Sites for Accessibility for Persons with Disabilities. *Journal of Disability Policy Studies*, *19*(1), 24–33. https://doi.org/10.1177/1044207308315274

Kausar, S., Tahir, B., & Mehmood, M. A. (2021, December). HashCat: A Novel Approach for the Topic Classification of Multilingual Twitter Trends. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 212–217). IEEE. https://doi.org/10.1109/fit53504.2021.00047

Kharismadewi, Y., Revita, I., & AS, R. M. (2023). A Praat-Based Stuttering Analysis of the Main Character in the King's Speech Movie: A Neuropsycholinguistic Study. *Journal of Applied Studies in Language*, *7*(1), 56–65. https://doi.org/10.31940/jasl.v7i1.56-65

Kous, K., Kuhar, S., Pavlinek, M., Heričko, M., & Pušnik, M. (2021). Web Accessibility Investigation of Slovenian Municipalities' Websites Before and After the Adoption of European Standard EN 301 549. *Universal Access in the Information Society*, *20*, 595–615. https://doi.org/10.1007/s10209-020-00732-9

Kous, K., Kuhar, S., Rajšp, A., & Šumak, B. (2020, September). Investigation of the Accessibility of Non-Text Content Published on Websites. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1645–1650). IEEE. https://doi.org/10.23919/mipro48935.2020.9245288

Krogh, K., & Johnson, J. (2006). A Life without Living: Challenging Medical and Economic Reductionism in Home Support Policy for People with Disabilities. In *D. Pothier, & R. Devlin (Eds.), Critical disability theory: Essays in philosophy, politics, policy and law* (pp. 151–176). Vancouver: University of British Columbia Press. https://doi.org/10.59962/9780774851695-010

Lister, K., Coughlan, T., Iniesto, F., Freear, N., & Devine, P. (2020, April). Accessible Conversational User Interfaces: Considerations for Design. In *Proceedings of the 17th International Web for All Conference* (pp. 1–11). https://doi.org/10.1145/3371300.3383343

Lowndes, A. M., & Connelly, D. M. (2023). User Experiences of Older Adults Navigating an Online Database of Community-Based Physical Activity Programs. *Digital Health*, *9*. https://doi.org/10.1177/20552076231167004

Matthews, C. K., & Harrington, N. G. (2000). Invisible disabilities. In *D.O. Braithwaite, & T. L. Thompson (Eds.), Handbook of Communication and People with Disabilities: Research and Application* (pp. 405–421). New Jersey: Lawrence Erlbaum Associates, Inc.

McCauley, J. B., Pickles, A., Huerta, M., & Lord, C. (2020). Defining Positive Outcomes in More and Less Cognitively Able Autistic Adults. *Autism Research*, *13*(9), 1548–1560. https://doi.org/10.1002/aur.2359

McKee, E., Popiel, M., & Boyce, W. (2006). *Policies and Programs to Facilitate Labour Force Participation for People with Episodic Disabilities: Recommendations for a Canadian Context Based on an International Analysis*. Toronto: Canadian Working Group on HIV and Rehabilitation.

Michelsanti, D., Tan, Z. H., Zhang, S. X., Xu, Y., Yu, M., Yu, D., & Jensen, J. (2021). An Overview of Deep-Learning-Based Audio-Visual Speech Enhancement and Separation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *29*, 1368–1396. https://doi.org/10.1109/taslp.2021.3066303

Mollow, A. (2010). When Black Women Start Going on Prozac. In *L. J. Davis (Ed). The Disability Studies Reader* (3d Ed., pp. 486–506). New York: Routledge.

Morgan, J. N. (2021). Policing Under Disability Law. *Stanford Law Review*, *73*, 1401–1469.

Mostafa, M. (2014). Architecture for Autism: Autism ASPECTSS™ in School Design. *International Journal of Architectural Research: ArchNet-IJAR*, *8*(1), 143–158. https://doi.org/10.26687/archnet-ijar.v8i1.314

Murphy, K. L. (2020). Civil Rights Laws: Americans With Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973. *Journal of Physical Education, Recreation & Dance*, *92*(1), 57–59. https://doi.org/10.1080/07303084.2021.1844555

Nath, H. K., & Liu, L. (2017). Information and Communications Technology (ICT) and Services Trade. *Information Economics and Policy*, *41*, 81–87. https://doi.org/10.1016/j.infoecopol.2017.06.003

Neely, B. H., & Hunter, S. T. (2014). In a Discussion on Invisible Disabilities, Let Us Not Lose Sight of Employees on the Autism Spectrum. *Industrial and Organizational Psychology*, *7*(2), 274–277. https://doi.org/10.1111/iops.12148

Olalere, A., & Lazar, J. (2011). Accessibility of US Federal Government Home Pages: Section 508 Compliance and Site Accessibility Statements. *Government Information Quarterly*, *28*(3), 303–309. https://doi.org/10.1016/j.giq.2011.02.002

Panda, S., & Chakravarty, R. (2020). Evaluating the Web Accessibility of IIT Libraries: A Study of Web Content Accessibility Guidelines. *Performance Measurement and Metrics*, *21*(3), 121–145. https://doi.org/10.1108/pmm-02-2020-0011

Patton, E. (2022). To Disclose or Not Disclose a Workplace Disability to Coworkers: Attributions and Invisible Health Conditions in the Workplace. *Equality, Diversity and Inclusion: An International Journal*, *41*(8), 1154–1180. https://doi.org/10.1108/edi-09-2021-0228

Pham, M., Singh, K., & Jahnke, I. (2023). Socio-Technical-Pedagogical Usability of Online Courses for Older Adult Learners. *Interactive Learning Environments*, *31*(5), 2855–2871. https://doi.org/10.1080/10494820.2021.1912784

Prince, M. J. (2017). Persons with Invisible Disabilities and Workplace Accommodation: Findings from a Scoping Literature Review. *Journal of Vocational Rehabilitation*, *46*(1), 75–86. https://doi.org/10.3233/jvr-160844

Proença, M. D. Q., Motti, V. G., Rodrigues, K. R. D. H., & Neris, V. P. D. A. (2021). Coping with Diversity-A System for End-users to Customize Web User Interfaces. *Proceedings of the ACM on Human-Computer Interaction*, *5*(EICS), 1–27. https://doi.org/10.1145/3457151

Reeve, T., & Gottselig, S. (2011). *Investigating Workplace Accommodation for People with Invisible Disabilities, Research Report*. Vancouver: BC Coalition of People with Disabilities.

Schall, C. M. (1998). The Americans with Disabilities Act – are we keeping our promise? An analysis of the effect of the ADA on the employment of persons with disabilities. *Journal of Vocational Rehabilitation*, *10*(3), 191–203. https://doi.org/10.3233/jvr-1998-10303

Schoen, J. (2022). Patching Procedural Potholes in Supplemental Jurisdiction Claims Involving ADA & Unruh Act Litigation in California Federal Courts. *Loyola Law Review*, *55*(4), 1107–1132. https://clck.ru/36kuXG

Seo, K., Dodson, S., Harandi, N. M., Roberson, N., Fels, S., & Roll, I. (2021). Active Learning with Online Video: The Impact of Learning Context on Engagement. *Computers & Education*, *165*, 104132. https://doi.org/10.1016/j.compedu.2021.104132

Shriberg, L. D., Kwiatkowski, J., & Mabie, H. L. (2019). Estimates of the Prevalence of Motor Speech Disorders in Children with Idiopathic Speech Delay. *Clinical Linguistics & Phonetics*, *33*(8), 679–706. https://doi.org/10.1080/02699206.2019.1595731

Smith, I. C., & White, S. W. (2020). Socio-Emotional Determinants of Depressive Symptoms in Adolescents and Adults with Autism Spectrum Disorder: A Systematic Review. *Autism*, *24*(4), 995–1010. https://doi.org/10.1177/1362361320908101

Taylor, Z. W., & Bicak, I. (2021). Two-Year Institution and Community College Web Accessibility: Updating the Literature After the 2018 Section 508 amendment. In *Graduate Students' Research about Community Colleges* (pp. 125–135). Routledge. https://doi.org/10.4324/9781003011392-10

Teh, Y. F., & Ramli, S. N. (2023). Implementation of Multi-Factor Authentication on A Vaccination Record System. *Applied Information Technology and Computer Science*, *4*(1), 19–39. https://doi.org/10.30880/aitcs.2023.04.01.002

Thompson, K. M., & Copeland, C. (2020). Inclusive Considerations for Optimal Online Learning in Times of Disasters and Crises. *Information and Learning Sciences*, *121*(7/8), 481–486. https://doi.org/10.1108/ils-04-2020-0083

van Rensburg, M. J., Weaver, C., Jenkins, C., Banister, M., King, E., & Bell, S. (2020). Using an Advocacy Practicum to Establish a Framework for Virtual Community Consultations in the Ottawa Adult Autism Community. In *Transforming Social Work Field Education* (p. 227). https://doi.org/10.2307/j.ctv3405pqj.18

Vickers, W., Reddivari, S., & Reddivari, K. (2022, August). Evaluating Audio-to-Text utilizing Dragon in the Context of Just-in-Time Requirements. In *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)* (pp. 124–125). IEEE. https://doi.org/10.1109/iri54793.2022.00037

Willmore, B. D., & King, A. J. (2023). Adaptation in Auditory Processing. *Physiological Reviews*, *103*(2), 1025–1058. https://doi.org/10.1152/physrev.00011.2022

Zhang, S., & Balog, K. (2020). Web Table Extraction, Retrieval, and Augmentation: A Survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *11*(2), 1–35. https://doi.org/10.1145/3372117

Zubala, A., Kennell, N., & Hackett, S. (2021). Art Therapy in the Digital World: An Integrative Review of Current Practice and Future Directions. *Frontiers in Psychology*, *12*, 595536. https://doi.org/10.3389/fpsyg.2021.600070

Žuliček, L., Tomić, S., & Bosnić, I. (2021, September). Adapting Modularized Web Applications to Web Accessibility Standards. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 470–475). IEEE. https://doi.org/10.23919/mipro52101.2021.9596750

Сведения об авторах

Хатсон Джеймс – PhD, заведующий кафедрой, ведущий специалист в области дополненной реальности, Университет Линденвуд
Адрес: МО 63301, США, г. Сент-Чарльз, ул. С. Кингшайвей, 209
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052

Хатсон Пайпер – доктор педагогики, преподаватель, Университет Линденвуд
Адрес: МО 63301, США, г. Сент-Чарльз, ул. С. Кингшайвей, 209
E-mail: phutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-1787-6143

Вклад авторов

Джеймс Хатсон осуществлял составление черновика рукописи и его критический пересмотр с внесением ценных замечаний интеллектуального содержания; разработку дизайна методологии; проведение сравнительного анализа; сбор литературы; анализ законодательства Соединенных Штатов Америки; подготовку и редактирование текста статьи; формулировку ключевых выводов, предложений и рекомендаций; оформление рукописи.
Пайпер Хатсон осуществляла формулирование идеи, исследовательских целей и задач; участие в научном дизайне; анализ и обобщение литературы; анализ законодательства Соединенных Штатов Америки; интерпретацию частных результатов исследования; критический пересмотр и редактирование текста рукописи; интерпретацию общих результатов исследования; утверждение окончательного варианта статьи.

Конфликт интересов

Авторы заявляют 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: 10.67.91 / Право социального обеспечения в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 10 августа 2023 г.
Дата одобрения после рецензирования – 20 сентября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.37

Digital Inclusion for People with Autism Spectrum Disorders: Review of the Current Legal Models and Doctrinal Concepts

James Hutson
Lindenwood University
Saint Charles, United States

Piper Hutson
Lindenwood University
Saint Charles, United States

Keywords

autism,
accessible environment,
legislation,
disability,
law,
autism spectrum disorder,
social security,
digital accessibility,
digital inclusion,
digital technologies

Abstract

Objective: today, a significant part of professional tasks are performed in the digital environment, on digital platforms, in virtual and other meetings. This necessitates a critical reflection of traditional views on the problem of accessible environment and digital accessibility, taking into account the basic universal needs of persons with disabilities.

Methods: a gap between the traditional legal perspective on special working conditions for persons with disabilities and the urgent need of a digital workplace (digital environment) clearly shows lacunas in the understanding of accessibility, which are identified and explored with formal-legal and doctrinal methods. The multifaceted aspects of digital inclusion are revealed based on an informative approach to legislation. It leads, among other things, to searching for recommendations which would fill this gap and contribute to the creation of a more inclusive and responsible legal, social and technological environment.

✉ Corresponding author

Results: the research has led to a conclusion that the existing legal, social and technological paradigms need to be re-evaluated. This reevaluation should aim to develop a more inclusive and benevolent concept of accessible environment that takes into account the diversity of human experience and needs, and a wide range of behavioral and cognitive characteristics. Creating special conditions in the workplace for those with overt and covert health problems should become an integral part of the employer's focus, along with improving management efficiency.

Scientific novelty: covert (hidden) health problems have traditionally been understudied, although they include a range of mental and physical impairments, which, like explicit health problems, vary in their origin, intensity, and permanent or episodic character. This study fills a gap in the issues of disability and its legal protection, taking into account the trend of digital inclusion, the dynamic labor activity of today, and the wide range of human abilities and needs.

Practical significance: the aspects of hidden or latent disability considered in the study provide a different perspective at employment, focusing on the workplace conditions that could be created. Employers may be unaware of the need to create special working conditions for those with hidden health problems. This results in negative effects on unemployment, increased sick leave, limited opportunities in the workplace, and more. Employees are often reluctant to disclose their non-obvious health problems to employers; hence, employers should facilitate disclosure of such information by creating relevant conditions. Such an approach will contribute to the legal protection of this category of employees and to further development of the existing legislative regulation, since the latter does not fully comply with today's needs and changed reality.

For citation

Hutson, J., & Hutson, P. (2023). Digital Inclusion for People with Autism Spectrum Disorders: Review of the Current Legal Models and Doctrinal Concepts. *Journal of Digital Technologies and Law, 1*(4), 851–879. https://doi.org/10.21202/jdtl.2023.37

References

Baptista, J., Stein, M. K., Klein, S., Watson-Manheim, M. B., & Lee, J. (2020). Digital Work and Organisational Transformation: Emergent Digital/Human Work Configurations in Modern Organisations. *The Journal of Strategic Information Systems*, *29*(2), 101618. https://doi.org/10.1016/j.jsis.2020.101618

Blanco, M., Zong, J., & Satyanarayan, A. (2022). *Olli: An Extensible Visualization Library for Screen Reader Accessibility*. https://vis.mit.edu/pubs/olli.pdf

Bosio, E., Djankov, S., Glaeser, E., & Shleifer, A. (2022). Public Procurement in Law and Practice. *American Economic Review*, *112*(4), 1091–1117. https://doi.org/10.1257/aer.20200738

Brooks, A. (2017). Accessibility: Definition, Labeling, and CVAA Impact. *Recent Advances in Technologies for Inclusive Well-Being: From Worn to Off-body Sensing, Virtual Worlds, and Games for Serious Applications*, 283–383. https://doi.org/10.1007/978-3-319-49879-9_14

Burks, C. L. (2013). Improving Access to Commercial Websites Under the Americans with Disabilities Act and the Twenty-First Century Communications and Video Accessibility Act. *Iowa Law Review, 99*(1), 363. https://clck.ru/36kuL4

Caldwell, B., Cooper, M., Reid, L. G., Vanderheiden, G., Chisholm, W., Slatin, J., & White, J. (2008). *Web Content Accessibility Guidelines (WCAG) 2.0. WWW Consortium (W3C)*, *290*, 1–34. https://clck.ru/36kuNe

Capuano, A. (2022). Post-Pandemic Workplace Design and the Plight of Employees with Invisible Disabilities: In Australian Labour Law and Anti-Discrimination Legislation Equipped to Address New and Emerging Workplace Inequalities?. *The University of New South Wales Law Journal*, *45*(2), 873–913. https://doi.org/10.53637/emwr6179

Chiou, P. T., Alotaibi, A. S., & Halfond, W. G. (2021, August). Detecting and Localizing Keyboard Accessibility Failures in Web Applications. In *Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering* (pp. 855–867). https://doi.org/10.1145/3468264.3468581

Clouse, J. R., Wood-Nartker, J., & Rice, F. A. (2020). Designing Beyond the Americans with Disabilities Act (ADA): Creating an Autism-Friendly Vocational Center. *HERD: Health Environments Research & Design Journal*, *13*(3), 215–229. https://doi.org/10.1177/1937586719888502

de Melo, F. D. A. F., Soares, K. P., de Barros, E. M., dos Santos Cabral, E. L., da Costa Júnior, J. F., da Silva, A. A. R. S., & Burlamaqui, A. M. F. (2022). Inclusive Digital Technologies in the Classroom: A Case Study Focused on Students with Autism Spectrum Disorder (ASD) in the Final Years of Elementary School. *Research, Society and Development*, *11*(6), e10211628759-e10211628759. https://doi.org/10.33448/rsd-v11i6.28759

Duarte, C., & Fonseca, M. J. (2019). *Multimedia Accessibility. In Web Accessibility: A Foundation for Research* (pp. 461–475). Springer, London. https://doi.org/10.1007/978-1-4471-7440-0_25

Farbenblum, B., & Berg, L. (2017). Migrant Workers' Access to Remedy for Exploitation in Australia: The Role of the National Fair Work Ombudsman. *Australian Journal of Human Rights*, *23*(3), 310–331. https://doi.org/10.1080/1323238x.2017.1392478

Fayyaz, N., & Khusro, S. (2023). Enhancing Accessibility for the Blind and Visually Impaired: Presenting Semantic Information in PDF Tables. *Journal of King Saud University – Computer and Information Sciences*, 101617. https://doi.org/10.1016/j.jksuci.2023.101617

Ferlazzo, E., Sueri, C., Masnou, P., Aguglia, U., Mercuri, S., Caminiti, E., & Piccioli, M. (2021). Technical Issues for Video Game Developers and Architects to Prevent Photosensitivity. In *The Importance of Photosensitivity for Epilepsy* (pp. 407–412). Springer, Cham. https://doi.org/10.1007/978-3-319-05080-5_33

Frey, B. A., & Mancilla, R. (2023). Inclusive Online Learning: Digital Accessibility Practices. In *Diversity in Higher Education Remote Learning: A Practical Guide* (pp. 93–104). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-31214-4_8

Gleason, C., Pavel, A., McCamey, E., Low, C., Carrington, P., Kitani, K. M., & Bigham, J. P. (2020, April). Twitter A11y: A Browser Extension to Make Twitter Images Accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1–12). https://doi.org/10.1145/3313831.3376728

Griffen, B., Woods-Catterlin, L., Lorah, E. R., & Whitby, P. S. (2022). Teaching Communication to Individuals with Autism Spectrum Disorders. In *Autism Spectrum Disorders: Advancing Positive Practices in Education.* (5th Ed.). Routledge. https://doi.org/10.4324/9781003255147-9

Hawkins, D. S. (2023). Overlooked and Undercounted: Communication and Police Brutality Against People with Disabilities. In *The Palgrave Handbook of Disability and Communication* (pp. 385–399). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-14447-9_23

Higgins, J. M., Arnold, S. R., Weise, J., Pellicano, E., & Trollor, J. N. (2021). Defining Autistic Burnout Through Experts by Lived Experience: Grounded Delphi Method Investigating #AutisticBurnout. *Autism*, *25*(8), 2356–2369. https://doi.org/10.1177/13623613211019858

Hodges, H., Fealko, C., & Soares, N. (2020). Autism Spectrum Disorder: Definition, Epidemiology, Causes, and Clinical Evaluation. *Translational Pediatrics*, *9*(Suppl 1), S55. https://doi.org/10.21037/tp.2019.09.09

Hurley-Hanson, A. E., Giannantonio, C. M., Griffiths, A. J., Hurley-Hanson, A. E., Giannantonio, C. M., & Griffiths, A. J. (2020). The Stigma of Autism. *Autism in the Workplace: Creating Positive Employment and Career Outcomes for Generation A* (pp. 21–45). https://doi.org/10.1007/978-3-030-29049-8_2

Hutson, P., & Hutson, J. (2023). Neurodiversity and Inclusivity in the Workplace: Biopsychosocial Interventions for Promoting Competitive Advantage. *Journal of Organizational Psychology*, *23*(2), 1–16. https://doi.org/10.33423/jop.v23i2.6159

Inal, Y., Guribye, F., Rajanen, D., Rajanen, M., & Rost, M. (2020, October). Perspectives and practices of digital accessibility: A survey of user experience professionals in Nordic countries. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society* (pp. 1–11). https://doi.org/10.1145/3419249.3420119

Maruthy, S., & Kelkar, P. (Eds.). (2023). *Understanding and Managing Fluency Disorders: From Theory to Practice*. Routledge. https://doi.org/10.4324/9781003367673

Jaeger, P. T. (2008). User-Centered Policy Evaluations of Section 508 of the Rehabilitation Act: Evaluating E-Government Web Sites for Accessibility for Persons with Disabilities. *Journal of Disability Policy Studies*, *19*(1), 24–33. https://doi.org/10.1177/1044207308315274

Kausar, S., Tahir, B., & Mehmood, M. A. (2021, December). HashCat: A Novel Approach for the Topic Classification of Multilingual Twitter Trends. In *2021 International Conference on Frontiers of Information Technology (FIT)* (pp. 212–217). IEEE. https://doi.org/10.1109/fit53504.2021.00047

Kharismadewi, Y., Revita, I., & AS, R. M. (2023). A Praat-Based Stuttering Analysis of the Main Character in the King's Speech Movie: A Neuropsycholinguistic Study. *Journal of Applied Studies in Language*, *7*(1), 56–65. https://doi.org/10.31940/jasl.v7i1.56-65

Kous, K., Kuhar, S., Pavlinek, M., Heričko, M., & Pušnik, M. (2021). Web Accessibility Investigation of Slovenian Municipalities' Websites Before and After the Adoption of European Standard EN 301 549. *Universal Access in the Information Society*, *20*, 595–615. https://doi.org/10.1007/s10209-020-00732-9

Kous, K., Kuhar, S., Rajšp, A., & Šumak, B. (2020, September). Investigation of the Accessibility of Non-Text Content Published on Websites. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1645–1650). IEEE. https://doi.org/10.23919/mipro48935.2020.9245288

Krogh, K., & Johnson, J. (2006). A Life without Living: Challenging Medical and Economic Reductionism in Home Support Policy for People with Disabilities. In *D. Pothier, & R. Devlin (Eds.), Critical disability theory: Essays in philosophy, politics, policy and law* (pp. 151–176). Vancouver: University of British Columbia Press. https://doi.org/10.59962/9780774851695-010

Lister, K., Coughlan, T., Iniesto, F., Freear, N., & Devine, P. (2020, April). Accessible Conversational User Interfaces: Considerations for Design. In *Proceedings of the 17th International Web for All Conference* (pp. 1–11). https://doi.org/10.1145/3371300.3383343

Lowndes, A. M., & Connelly, D. M. (2023). User Experiences of Older Adults Navigating an Online Database of Community-Based Physical Activity Programs. *Digital Health*, *9*. https://doi.org/10.1177/20552076231167004

Matthews, C. K., & Harrington, N. G. (2000). Invisible disabilities. In *D.O. Braithwaite, & T. L. Thompson (Eds.), Handbook of Communication and People with Disabilities: Research and Application* (pp. 405–421). New Jersey: Lawrence Erlbaum Associates, Inc.

McCauley, J. B., Pickles, A., Huerta, M., & Lord, C. (2020). Defining Positive Outcomes in More and Less Cognitively Able Autistic Adults. *Autism Research*, *13*(9), 1548–1560. https://doi.org/10.1002/aur.2359

McKee, E., Popiel, M., & Boyce, W. (2006). *Policies and Programs to Facilitate Labour Force Participation for People with Episodic Disabilities: Recommendations for a Canadian Context Based on an International Analysis*. Toronto: Canadian Working Group on HIV and Rehabilitation.

Michelsanti, D., Tan, Z. H., Zhang, S. X., Xu, Y., Yu, M., Yu, D., & Jensen, J. (2021). An Overview of Deep-Learning-Based Audio-Visual Speech Enhancement and Separation. *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, *29*, 1368–1396. https://doi.org/10.1109/taslp.2021.3066303

Mollow, A. (2010). When Black Women Start Going on Prozac. In *L. J. Davis (Ed). The Disability Studies Reader* (3d Ed., pp. 486–506). New York: Routledge.

Morgan, J. N. (2021). Policing Under Disability Law. *Stanford Law Review*, *73*, 1401–1469.

Mostafa, M. (2014). Architecture for Autism: Autism ASPECTSS™ in School Design. *International Journal of Architectural Research: ArchNet-IJAR*, *8*(1), 143–158. https://doi.org/10.26687/archnet-ijar.v8i1.314

Murphy, K. L. (2020). Civil Rights Laws: Americans With Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973. *Journal of Physical Education, Recreation & Dance*, *92*(1), 57–59. https://doi.org/10.1080/07303084.2021.1844555

Nath, H. K., & Liu, L. (2017). Information and Communications Technology (ICT) and Services Trade. *Information Economics and Policy*, *41*, 81–87. https://doi.org/10.1016/j.infoecopol.2017.06.003

Neely, B. H., & Hunter, S. T. (2014). In a Discussion on Invisible Disabilities, Let Us Not Lose Sight of Employees on the Autism Spectrum. *Industrial and Organizational Psychology*, *7*(2), 274–277. https://doi.org/10.1111/iops.12148

Olalere, A., & Lazar, J. (2011). Accessibility of US Federal Government Home Pages: Section 508 Compliance and Site Accessibility Statements. *Government Information Quarterly*, *28*(3), 303–309. https://doi.org/10.1016/j.giq.2011.02.002

Panda, S., & Chakravarty, R. (2020). Evaluating the Web Accessibility of IIT Libraries: A Study of Web Content Accessibility Guidelines. *Performance Measurement and Metrics*, *21*(3), 121–145. https://doi.org/10.1108/pmm-02-2020-0011

Patton, E. (2022). To Disclose or Not Disclose a Workplace Disability to Coworkers: Attributions and Invisible Health Conditions in the Workplace. *Equality, Diversity and Inclusion: An International Journal*, *41*(8), 1154–1180. https://doi.org/10.1108/edi-09-2021-0228

Pham, M., Singh, K., & Jahnke, I. (2023). Socio-Technical-Pedagogical Usability of Online Courses for Older Adult Learners. *Interactive Learning Environments*, *31*(5), 2855–2871. https://doi.org/10.1080/10494820.2021.1912784

Prince, M. J. (2017). Persons with Invisible Disabilities and Workplace Accommodation: Findings from a Scoping Literature Review. *Journal of Vocational Rehabilitation*, *46*(1), 75–86. https://doi.org/10.3233/jvr-160844

Proença, M. D. Q., Motti, V. G., Rodrigues, K. R. D. H., & Neris, V. P. D. A. (2021). Coping with Diversity-A System for End-users to Customize Web User Interfaces. *Proceedings of the ACM on Human-Computer Interaction*, *5*(EICS), 1–27. https://doi.org/10.1145/3457151

Reeve, T., & Gottselig, S. (2011). *Investigating Workplace Accommodation for People with Invisible Disabilities, Research Report*. Vancouver: BC Coalition of People with Disabilities.

Schall, C. M. (1998). The Americans with Disabilities Act – are we keeping our promise? An analysis of the effect of the ADA on the employment of persons with disabilities. *Journal of Vocational Rehabilitation*, *10*(3), 191–203. https://doi.org/10.3233/jvr-1998-10303

Schoen, J. (2022). Patching Procedural Potholes in Supplemental Jurisdiction Claims Involving ADA & Unruh Act Litigation in California Federal Courts. *Loyola Law Review*, *55*(4), 1107–1132. https://clck.ru/36kuXG

Seo, K., Dodson, S., Harandi, N. M., Roberson, N., Fels, S., & Roll, I. (2021). Active Learning with Online Video: The Impact of Learning Context on Engagement. *Computers & Education*, *165*, 104132. https://doi.org/10.1016/j.compedu.2021.104132

Shriberg, L. D., Kwiatkowski, J., & Mabie, H. L. (2019). Estimates of the Prevalence of Motor Speech Disorders in Children with Idiopathic Speech Delay. *Clinical Linguistics & Phonetics*, *33*(8), 679–706. https://doi.org/10.1080/02699206.2019.1595731

Smith, I. C., & White, S. W. (2020). Socio-Emotional Determinants of Depressive Symptoms in Adolescents and Adults with Autism Spectrum Disorder: A Systematic Review. *Autism*, *24*(4), 995–1010. https://doi.org/10.1177/1362361320908101

Taylor, Z. W., & Bicak, I. (2021). Two-Year Institution and Community College Web Accessibility: Updating the Literature After the 2018 Section 508 amendment. In *Graduate Students' Research about Community Colleges* (pp. 125–135). Routledge. https://doi.org/10.4324/9781003011392-10

Teh, Y. F., & Ramli, S. N. (2023). Implementation of Multi-Factor Authentication on A Vaccination Record System. *Applied Information Technology and Computer Science*, *4*(1), 19–39. https://doi.org/10.30880/aitcs.2023.04.01.002

Thompson, K. M., & Copeland, C. (2020). Inclusive Considerations for Optimal Online Learning in Times of Disasters and Crises. *Information and Learning Sciences*, *121*(7/8), 481–486. https://doi.org/10.1108/ils-04-2020-0083

van Rensburg, M. J., Weaver, C., Jenkins, C., Banister, M., King, E., & Bell, S. (2020). Using an Advocacy Practicum to Establish a Framework for Virtual Community Consultations in the Ottawa Adult Autism Community. In *Transforming Social Work Field Education* (p. 227). https://doi.org/10.2307/j.ctv3405pqj.18

Vickers, W., Reddivari, S., & Reddivari, K. (2022, August). Evaluating Audio-to-Text utilizing Dragon in the Context of Just-in-Time Requirements. In *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)* (pp. 124–125). IEEE. https://doi.org/10.1109/iri54793.2022.00037

Willmore, B. D., & King, A. J. (2023). Adaptation in Auditory Processing. *Physiological Reviews*, *103*(2), 1025–1058. https://doi.org/10.1152/physrev.00011.2022

Zhang, S., & Balog, K. (2020). Web Table Extraction, Retrieval, and Augmentation: A Survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *11*(2), 1–35. https://doi.org/10.1145/3372117

Zubala, A., Kennell, N., & Hackett, S. (2021). Art Therapy in the Digital World: An Integrative Review of Current Practice and Future Directions. *Frontiers in Psychology*, *12*, 595536. https://doi.org/10.3389/fpsyg.2021.600070

Žuliček, L., Tomić, S., & Bosnić, I. (2021, September). Adapting Modularized Web Applications to Web Accessibility Standards. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 470–475). IEEE. https://doi.org/10.23919/mipro52101.2021.9596750

Authors information

James Hutson – PhD, Head of the Department, Lead XR Disruptor, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: jhutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-0578-6052

Piper Hutson – EdD, Lecturer, Lindenwood University
Address: 209 S. Kingshighway St, MO 63301, Saint Charles, United States
E-mail: phutson@lindenwood.edu
ORCID ID: https://orcid.org/0000-0002-1787-6143

Authors' contributions

James Hutson drafted the manuscript and critically revised it with valuable intellectual comments; developed the methodology design; conducted comparative analysis; collected literature; analyzed the United States legislation; drafted and edited the article; formulated the key findings, suggestions, and recommendations; and drafted the manuscript.
Piper Hutson formulated the idea, research objectives, and goals; participated in the research design; reviewed and summarized literature; analyzed the United States legislation; interpreted the specific and general research findings; critically reviewed and edited the manuscript; approved the final version of the article.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 10, 2023
Date of approval – September 20, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/wxwsvu
DOI: https://doi.org/10.21202/jdtl.2023.38

На пути к правовому регулированию генеративного ИИ в творческой индустрии

Наталья Игоревна Шумакова ✉

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Джордан Дж. Ллойд

Компания «Unseen History»
г. Эссекс, Великобритания

Елена Викторовна Титова

Южно-Уральский государственный университет (национальный исследовательский университет)
г. Челябинск, Российская Федерация

Ключевые слова

авторское право, генеративный искусственный интеллект, интеллектуальная собственность, искусственный интеллект, международное право, нейронная сеть, объект авторского права, субъект авторского права, творческая индустрия, цифровые технологии

Аннотация

Цель данной статьи – ответить на следующие вопросы: 1. Может ли генеративный искусственный интеллект быть субъектом авторского права? 2. К каким рискам может привести нерегулируемое использование систем генеративного искусственного интеллекта? 3. Какие правовые пробелы необходимо закрыть для минимизации таких рисков?

Методы: сравнительно-правовой анализ, социологический метод, частно-социологический метод, количественный и качественный анализ данных, статистический анализ, метод кейсов, индукция, дедукция.

Результаты: авторы выявили ряд рисков, возникающих при нерегулируемом использовании генеративного искусственного интеллекта в творческой индустрии, среди которых нарушение авторского и трудового права, нарушение прав потребителей и рост недоверия населения к власти. Авторы полагают, что оперативная разработка новых правовых норм может минимизировать эти риски. В заключение констатируется, что государства уже начали осознавать опасность игнорирования негативного влияния генеративного искусственного интеллекта на творческую индустрию, что обусловливает разработку аналогичных правовых норм в государствах с совершенно разными режимами.

✉ Контактное лицо

Научная новизна: в работе проведено комплексное исследование влияния генеративного искусственного интеллекта на творческую индустрию с двух точек зрения: с позиции права и с позиции индустрии. Эмпирическую базу составляют два международных исследования и экспертное мнение представителя отрасли. Такой подход позволил авторам повысить объективность исследования и получить результаты, которые могут быть использованы для поиска практического решения выявленных рисков. Проблема непрерывного развития и роста популярности систем генеративного искусственного интеллекта выходит за рамки вопроса «кто автор?», поэтому ее необходимо решать путем внедрения иных, нежели уже существующих, механизмов и правил. Данная точка зрения подтверждается не только результатами проведенных исследований, но и анализом текущих судебных исков к разработчикам систем генеративного искусственного интеллекта.

Практическая значимость: полученные результаты могут быть использованы для ускорения разработки универсальных правовых норм, правил, инструментов и стандартов, отсутствие которых в настоящее время представляет угрозу не только для прав человека, но и для ряда отраслей творческой индустрии и других областей.

Для цитирования

Шумакова, Н. И., Ллойд, Дж. Дж., Титова, Е. В. (2023). На пути к правовому регулированию генеративного ИИ в творческой индустрии. *Journal of Digital Technologies and Law*, *1*(4), 880–908. https://doi.org/10.21202/jdtl.2023.38

Содержание

Введение

В 2023 г. даже те, кто никогда не проявлял интереса к разработке систем генеративного искусственного интеллекта (далее – ИИ), столкнулись с результатами их негативного влияния на творческую индустрию. Причиной послужили забастовки Гильдии киноактеров и Американской федерации артистов телевидения и радио (SAG-AFTRA) и Гильдии сценаристов Америки (WGA), которые привели к задержке

выпуска долгожданных работ[1] и, как утверждается, могут в обозримом будущем изменить всю индустрию[2].

Можно с уверенностью сказать, что названные забастовки повлияли на отношение ученых и практиков в области юриспруденции к использованию генеративного ИИ: от попыток выяснить, можно ли рассматривать генеративный ИИ в качестве автора и как защитить продукты, созданные искусственным интеллектом (Wan & Lu, 2021), они перешли к изучению его влияния на материальное положение представителей творческих профессий (Sparkes, 2022) и обсуждению требований к ответственности систем генеративного ИИ (Díaz-Rodríguez et al., 2023).

Принимая во внимание результаты предыдущих исследований, авторы данной статьи выявили необходимость проведения всестороннего анализа возможных рисков, связанных с нерегулируемым использованием генеративного ИИ. Чтобы выяснить, действительно ли он представляет собой экзистенциальную угрозу[3] для творческой индустрии, был использован ряд междисциплинарных методов, проведено два опроса по этике использования генеративного ИИ в творческой индустрии и области культуры и получено мнение по данному вопросу представителя творческой индустрии. Все это определило тему данного исследования.

Статья состоит из двух глав: «Голос закона» и «Голос индустрии» – и отражает результаты проведенных опросов, статистику, результаты сравнительно-правового анализа, применения метода кейсов и т. д.

В заключение авторы констатируют, что, несмотря на отсутствие в настоящее время международного правового регулирования использования генеративных систем искусственного интеллекта в творческой индустрии, государства уже разрабатывают достаточно схожие между собой законодательные проекты, конечной целью которых является повышение ответственности компаний, производящих и/или владеющих генеративными системами искусственного интеллекта; при этом ключевыми моментами являются своевременные принятие и применение таких норм с целью снижения выявленных рисков и предотвращения возможного ущерба.

1. Голос закона

Попытки изобрести робота, способного создавать что-либо, не новы. Фактически первые роботы, имитирующие творческий процесс, появились более 500 лет назад, и сразу же возник вопрос, смогут ли они заменить настоящего человека[4]. В XVIII в. их называли автоматами и они были очень популярны; именно тогда Пьер Жаке-Дро создал свои знаменитые автоматы, которые рисовали картины, играли на музыкальных инструментах и развлекали публику другими способами, действуя по

1 Kelley, S. (2023, September 19). All the major movies and TV shows delayed by the strikes. Los Angeles Times. https://clck.ru/36n37w

2 Belloni, M., & Shaw, L. (2023, September 18). The Strike's Permanent Damage: Who Will Suffer the Most? The Ringer. https://clck.ru/36n38d

3 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

4 Marvellous machines: early robots. (2018, November 20). Science Museum. https://goo.su/Scuk

заложенной в них программе[5]. Будет справедливо сказать, что системы генеративного ИИ функционируют примерно так же, как те ранние роботы, – они делают то, на что их запрограммировали, применяя различные техники для создания продукта на основе данных, использованных во время их обучения. Тем не менее уже многие годы ученые задаются вопросом, не сильно отличающимся от того, что был задан три столетия назад: «Может ли генеративный ИИ быть творцом?» (Соменков, 2019). Как правило, за этим вопросом сразу же следует другой – «Могут ли продукты генеративного ИИ быть объектом прав интеллектуальной собственности и авторского права?» (Агибалова, Перекрёстова, 2020). Ответить на эти вопросы можно по-разному. Но уже одно это свидетельствует о том, что современный правовой статус генеративных систем ИИ остается неопределенным (Stokel-Walker, 2023). Здесь мы скорее согласны с той точкой зрения, что важнее решить вопрос взаимоотношений человека и машины в творческом процессе, а также вопрос о меняющемся характере круга заинтересованных сторон, вовлеченных в этот процесс, поскольку ответы на них можно найти в действующем законодательстве большинства стран (Fenwick & Jurčys, 2023). При этом стоит отметить, что есть и исключения, например, Китай и Новая Зеландия. Если посмотреть на иски и судебные решения в Китае, то можно заметить, что в этой стране практикуется неоднозначный подход к признанию объекта авторского права. Так, в работе Wan & Lu (2021) приводятся два примера: 1) в деле Beijing Film Law Firm vs. Beijing Baidu Netcom Science & Technology Co Ltd Пекинский интернет-суд пришел к выводу, что объект спора был полностью сгенерирован искусственным интеллектом и, следовательно, не может охраняться авторским правом; 2) в деле Shenzhen Tencent Computer System Co Ltd vs. Shanghai Yingxun Technology Co Ltd суд района Наньшань г. Шэньчжэнь проанализировал действия реального человека в процессе генерации объекта спора и постановил, что его результат подлежит охране в соответствии с Законом об авторском праве Китая. Новая Зеландия, в свою очередь, избрала совершенно иной подход. Согласно разделу «Интерпретация» Закона об авторском праве (1994 г.), «понятие ‘созданное компьютером’ применительно к произведению означает, что произведение создано компьютером в условиях, при которых человек как автор произведения отсутствует»[6], поэтому теоретически по логике этой нормы генеративный ИИ может быть субъектом авторского права, а его продукты – объектами авторского права. Однако ст. 5 «Значение авторства» не включает его в список возможных авторов; более того, в ней говорится, что «автором произведения является лицо, его создавшее»[7], что опять же вызывает неопределенность правового статуса генеративного ИИ.

В России пока не разработано специального правового регулирования использования генеративного ИИ в творческой индустрии, но для целей данного исследования важно изучить рекомендации и комментарии юристов и экспертов по вопросам защиты генерируемых продуктов. Одни специалисты настаивают на необходимости разработки новых механизмов и институтов, позволяющих контролировать

5 DNA. Jaquet Droz. https://clck.ru/36nqDJ

6 Copyright Act 1994 No. 143. Version as at 31 May 2023. (2023). Parliamentary Council Office. https://clck.ru/36n3Ds

7 Там же.

генеративные системы искусственного интеллекта[8]; другие считают существующие правовые нормы достаточными для ответа на новые вызовы, связанные с развитием названных технологий и их использованием[9]. Имеющиеся открытые источники также дают интересные рекомендации для бизнеса по использованию генеративных систем искусственного интеллекта. Так, А. Семенов (IT Moscow Digital School) считает, что продукты, генерируемые искусственным интеллектом, не являются объектами авторского права, а значит, могут свободно использоваться в коммерческих целях[10]. Ю. Брисов (Digital & Analogue Partners) представляет противоположную точку зрения и рекомендует внимательно изучать условия, установленные создателями конкретной системы генеративного ИИ, поскольку, согласно им, субъектами авторского права могут быть не пользователи, а владельцы или создатели такой системы, и это относится не только к использованию российских генеративных систем ИИ[11]. Например, YandexArt ограничивает любое коммерческое использование изображений и текстов, сгенерированных с помощью их системы; кроме того, продукты, сгенерированные в приложении «Шедеврум», могут быть использованы в коммерческих целях самой компанией[12]. При этом, как ни странно, в пресс-релизе упомянутого приложения такой информации нет, более того, он производит прямо противоположное впечатление[13].

Юристы из США и Великобритании также высказывали свое мнение по этому вопросу. Юридическая фирма Джозефа Савери на своей официальной странице утверждает, что продукты, созданные с использованием Stable Diffusion, DreamStudio, DreamUp и Midjourney, «нарушают права тысяч художников и творцов» и фактически накладывают «финансовую нагрузку»[14]. Это мнение совпадает с комментарием D. Lee (BDB Pitmans), в котором он подчеркивает, что даже отсутствие адекватной терминологии в случае использования генеративных систем ИИ может нанести вред. Юрист также указывает, что может быть «непросто» продемонстрировать конкретный вред из-за специфики процесса обучения таких систем. Кроме того, он предполагает, что использование генеративных систем искусственного интеллекта может нарушать права авторов, на произведениях которых эти системы обучались, поскольку «несанкционированное использование их произведений искусственным интеллектом может изменить их смысл, тем самым нанеся ущерб их репутации или художественной ценности произведения» (право оспаривать уничижительное обращение с произведением). Автор также добавляет, что в соответствии с действующим

8 Reshetnikova, A. (2019, October 29). Творец или инструмент в руках автора? Advokatskaya Gazeta. https://clck.ru/36n3Ge

9 Головоломка: взгляд юристов на искусственный интеллект. (2023, April 20). Advokatskaya Gazeta. https://clck.ru/36n3HJ

10 Kildyushkin, R. (2022, July 13). Стало известно, кому принадлежат авторские права на созданные нейросетями картинки. Gazeta.ru. https://goo.su/ER4l

11 Brisov, Yu. (2023, May 25). Можно ли использовать творчество нейросетей в бизнесе? Bisnes Secrety. https://clck.ru/36n3KB

12 Terms of us of Shedevrum. Yandex. https://clck.ru/3663j8

13 YandexArt. Ya.ru. https://clck.ru/36n3L9

14 AI Image Generator – Copyright Litigation. Joseph Savery Law Firm. https://clck.ru/36n3LZ

законодательством использование материалов, защищенных авторским правом, для обучения генеративного ИИ может рассматриваться как «правомерное»[15].

Особое мнение имеет Бюро по авторским правам США. Согласно их решению от 21 февраля 2023 г., произведения, созданные искусственным интеллектом, не могут быть объектом авторского права. Более того, они отменили первоначальную регистрацию произведения, созданного с использованием Midjourney (комикс Кристины Каштановой), и признали объектом авторского права только его текст и «отбор, согласование и расположение текста, созданного автором», но не сгенерированные изображения[16]. Апелляционный суд Великобритании занимает аналогичную позицию. Согласно его недавнему решению, генеративные системы искусственного интеллекта не могут быть изобретателями и, следовательно, их продукты не могут считаться объектами патентного права[17].

Нельзя обойти вниманием и позицию Австралии по отношению к использованию генеративных систем ИИ. Так, правительство Э. Албанезе считает генеративные системы ИИ экзистенциальной угрозой из-за их способности создавать «дипфейки», распространять дезинформацию и влиять на демократические процессы другими способами, поэтому в последнее время обсуждается вопрос об их запрете или постановке под контроль[18]. Между тем, согласно недавнему исследованию, проведенному компанией BlackBerry Limited, 93 % австралийских компаний в настоящее время вводят или рассматривают возможность введения запрета на использование систем генеративного ИИ на рабочих местах, поскольку считают их угрозой как для безопасности, так и для репутации[19]. В своем исследовании[20] BlackBerry Limited также показала, что эта тенденция является глобальной и 75 % компаний по всему миру разделяют точку зрения австралийцев на подобные цифровые технологии, хотя и признают, что они могут быть полезным инструментом.

Чтобы понять возможные негативные последствия использования генеративных систем ИИ, два комитета Палаты общин провели комплексные расследования, результаты которых были представлены в начале этого года[21, 22]. В обоих была выявлена реальная возможность нарушения авторских прав, прав интеллектуальной собственности, трудового законодательства, а также угроза массового производства дезинформации, дипфейков и другого противоправного контента, в случае если в ближайшее время не будут устранены существующие правовые пробелы,

---

15 AI authors – what a US lawsuit could mean for UK IP law. (2023, August 10). The Trademark Lawyer. https://clck.ru/36n3PR

16 Re: Zarya of the Dawn (Registration # VAu001480196). (2023, February 21). United States Copyright Office. https://clck.ru/36n3Pk

17 Neutral Citation Number: [2021] EWCA Civ 1374 Case No: A3/2020/1851. British and Irish Legal Information Institute. https://clck.ru/36n3Qb

18 Safe and responsible AI. (2023, June 1). Ministry for Industry and Science. https://goo.su/rs4z

19 Organisations in Australia set to ban ChatGPT and generative AI apps on work devices. APDR – Asia-Pasific Defense Reporter. (2023, August 14). https://clck.ru/36KzWP

20 Why Are So Many Organizations Banning ChatGPT? (2023, August 8). BlackBerry. https://clck.ru/36n3S4

21 UK Parliament. (2023). Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. https://clck.ru/36n3Sf

22 UK Parliament. (2023). The governance of artificial intelligence: interim report: Ninth Report of Session 2022–23. https://clck.ru/36n3TN

в том числе в абстрактной терминологии. В целом рекомендации, представленные в первом отчете[23], совпадают с рекомендациями британского Агентства по вопросам интеллектуальной собственности – необходимо изменить законодательство Великобритании, чтобы адекватно реагировать на вызовы, связанные с развитием цифровых технологий[24]. По результатам названных исследований был сформулирован перечень социальных издержек, к которым может привести нерегулируемое использование генеративных систем ИИ. Среди таких ущербов назовем деградацию информационной среды, дезорганизацию рынка труда, предвзятость и репутационные издержки[25].

Тем не менее на сегодняшний день Китай является единственной страной, которая уже регулирует использование генеративных систем искусственного интеллекта, что обусловливает важность анализа подходов к их использованию. Документ «Временные меры по управлению сервисами генеративного искусственного интеллекта», вступивший в силу этом году, в ст. 7 обязывает обучать системы генеративного искусственного интеллекта только на данных, полученных с соблюдением этики, чтобы предотвратить возможное нарушение авторских прав или прав интеллектуальной собственности, а в ст. 12 обязывает поставщиков услуг генеративного искусственного интеллекта ставить на свои продукты соответствующую маркировку[26]. Китайские юристы поясняют, что, согласно новым правилам, провайдеры также обязаны маркировать данные, используемые в процессе исследований и разработок[27], и утверждают, что при разработке этих мер было учтено мнение общественности[28]. А для того чтобы введенные правила заработали, Национальный технический комитет по стандартизации информационной безопасности выпустил «Руководство по стандартной практике сетевой безопасности – метод идентификации контента сервисов генеративного искусственного интеллекта», в котором подробно описано, как должны маркироваться продукты генеративного искусственного интеллекта и зачем это нужно делать[29]. Таким образом, можно утверждать, что Китай является пионером в области правового регулирования использования систем генеративного искусственного интеллекта.

2. Голос индустрии

Анализ современных попыток регулировать использование генеративных систем искусственного интеллекта показывает, что Великобритания и Китай стараются учитывать голос индустрий (как творческих, так и кибернетических) и потребителей их продукции. Действительно, голос человека-творца в последнее время стал слышен настолько

---

23 UK Parliament. (2023). Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. https://clck.ru/36n3Sf

24 IPO Transformation programme: second consultation. (2023, August 22). GOV.UK. https://clck.ru/36n3zQ

25 AI safety summit. Department For Science, Innovation and Technology. https://clck.ru/36n3zq

26 生成式人工智能服务管理暂行办法 от 1994 № 143 // 国家互联网信息办公室. (2023). – 第15号 10.07.2023. https://goo.su/fbbG

27 Regulatory and legislation: China's Interim measures for the Management of Generative Artificial Intelligence Services officially implemented. (2023, August). 普华永道中国. https://clck.ru/36n43s

28 Cai, R., & Zhu, W. (2023, July 14). Comparative Analysis of China's New Generative AI Regulations. Zhong Lun. https://clck.ru/36n44e

29 网络安全标准实践指南—生成式人工智能服务内容标识方法 – 2023 № TC260-PG-20233A. (2023). 全国信息安全标准化技术委员会秘书处. https://goo.su/Gl6Shf1

громко, что даже Сенат США был вынужден к нему прислушаться[30]. Судебные иски, слушания в Конгрессе и, конечно, забастовки – все это можно считать признаками растущего общественного, а точнее политического, недоверия. И действительно, когда граждане той или иной страны чувствуют неуверенность в своем будущем (Küçükkömürler & Özkan, 2022), ощущают, что их «бросили» (Stroppe, 2023), или считают, что их правительство не в состоянии предпринять соответствующие правовые действия для снижения рисков, которые эти граждане рассматривают как возможную угрозу, тогда они склонны к таким действиям, как забастовки, протесты и митинги (Torres & Bellinger, 2014). Не способствует разрешению ситуации и то, что такие медиагиганты, как Time, публикуют информацию о лоббировании «смягчения европейских правил в области ИИ»[31] такими корпорациями, как OpenAI, и успехе этого лоббирования[32]. Более того, создается впечатление, что обычные переговорщики, вся цель существования которых заключается в представлении законных интересов творческой индустрии, поступают прямо противоположным образом[33]. Кроме того, лидеры мнений, такие как Алекс Винтер, также публично выражают свое политическое недоверие, обвиняя правительство в том, что оно «захвачено BigTech», и называя The People's Summit[34] более важным, чем AI Safety Summit[35], который, по их мнению, только ухудшит ситуацию, поскольку правительства «не могут защитить своих граждан»[36]. Отсюда вытекает важность изучения мнений представителей творческой индустрии и потребителей ее продукции. В данной статье представлены результаты двух международных опросов, проведенных одним из соавторов – Джорданом Дж. Ллойдом (*далее его текст выделен курсивом*).

Опросы проводились в социальных сетях и мессенджере Telegram с 11 июля по 11 октября 2023 г.

География опросов:

103 из 117 англоязычных респондентов предоставили информацию о своем месте жительства. Судя по ответам, они представляют 21 страну: США, Великобританию, Аргентину, Канаду, Бельгию, Германию, Францию, Норвегию, Нидерланды, Турцию, Данию, ЮАР, Чили, Чехию, Сербию, Австралию, Австрию, Италию, Ирландию, Новую Зеландию, Швецию (рис. 1). Абсолютное большинство из них работает в творческой индустрии – 85,5 %, и только 14,5 % англоязычных респондентов являются потребителями ее продукции (рис. 2).

30 Artificial Intelligence and Intellectual Property – Part II: Copyright. Subcommittee on intellectual property. https://clck.ru/36n3aE

31 Big Tech Is Already Lobbying to Water Down Europe's AI Rules. Time. https://clck.ru/36n3ak

32 Exclusive: OpenAI Lobbied the E.U. to Water Down AI Regulation. Time. https://clck.ru/36n3bJ

33 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

34 The People's AI Summit – The citizens. YouTube. https://clck.ru/36n3cb

35 AI Safety Summit: introduction. GOV.UK. https://clck.ru/36n4AB

36 AI's threat to democracy and labour looms large. UK's 'doomsday' AI summit is poised to make things worse. Big Issue. https://clck.ru/36n3dx

Рис. 1

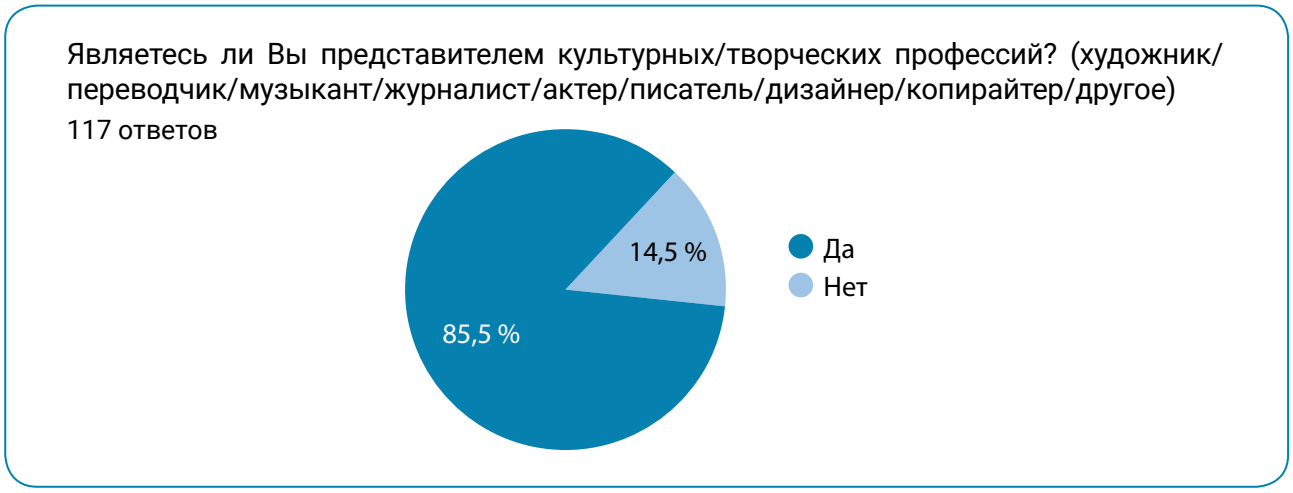


Рис. 2

31 из 36 русскоязычных респондентов также предоставили такую информацию, и, судя по их ответам, они представляют четыре страны: Россию – 90,4 %, Молдову – 3,2 %, Польшу – 3,2 % и Латвию – 3,2 %, причем абсолютное большинство из них также заняты в творческой индустрии – 72,2 %, а 27,8 % русскоязычных респондентов являются потребителями ее продукции.

Этика проведения опросов: опросы были анонимными; все респонденты были проинформированы о возможном использовании их ответов в научных целях.

2.1. Генеративный ИИ как субъект авторского права, продукты генеративного ИИ как объекты авторского права

В предыдущей главе мы установили, что ни у ученых, ни у законотворцев нет универсального понимания того, можно ли считать генеративный ИИ творцом. Г-н Ллойд излагает здесь свою точку зрения, согласно которой генеративный ИИ не может рассматриваться в качестве творца: «*Законодательство об авторском праве в его нынешнем виде распространяется на произведения, созданные в результате человеческой*

деятельности. Как отмечалось, создание запросов основано на человеческом воображении, но происходящий в результате этого процесс и созданный продукт таковыми не являются, поэтому не могут быть защищены авторским правом, если придерживаться преобладающей точки зрения. Я сравниваю генеративный ИИ с азартной игрой, такой как игровой автомат в казино. Вращение барабанов создает варианты, где вы можете зафиксировать определенные варианты, которые вам нравятся, а затем снова вращать барабан, чтобы достичь более желаемого результата. Примерно так же работают запросы при использовании генеративного ИИ». Вопрос, который всегда возникает при обсуждении правового статуса генеративного ИИ, заключается в том, можно ли защищать созданные с его помощью продукты как объекты авторского права и права интеллектуальной собственности. Опять же, как мы установили ранее, по букве закона в ряде стран это возможно. Но вопрос в том, следует ли это делать? «*Нет, или, по крайней мере, следует создать новую форму системы защиты авторских прав/интеллектуальной собственности (ИС), чтобы включить активы, созданные ИИ, как отдельный объект, отличный от объекта существующего авторского права. Действующая система авторского права не идеальна, но она хорошо отлажена и приносит пользу как авторам, так и компаниям, занимающимся ИС. Защита и возмещение, предлагаемые существующей системой, конечно, находятся под угрозой из-за наплыва активов, созданных искусственным интеллектом. Я где-то читал, что всего девять месяцев потребовалось для создания такого количества 'новых' произведений искусства, которое было создано за всю историю человечества. Очевидно, что законодательство в области авторского права и ИС должно действовать быстро, чтобы защитить авторов оригинальных произведений*».

Эти вопросы были заданы в ходе опросов, и их результаты явно свидетельствуют о том, что творческая индустрия и потребители ее продукции придерживаются единого мнения: 65 % англоязычных респондентов не считают, что продукты генеративного ИИ должны охраняться Законом об авторском праве (рис. 3), и столько же из них не считают, что продукты ИИ должны охраняться правами интеллектуальной собственности (рис. 4), тогда как 11,1 % ответили, что продукты, созданные с использованием ИИ, должны охраняться Законом об авторском праве (рис. 3), а 9,4 % предполагают, что такие продукты должны охраняться правами интеллектуальной собственности (рис. 4).

Рис. 3

Рис. 4

Русскоязычные респонденты отвечали на те же вопросы, и 61,1 % из них считают, что такие продукты не должны охраняться ни законом об авторском праве (рис. 5), ни правами интеллектуальной собственности (рис. 6). Однако 25 % русскоязычных респондентов считают, что продукты генеративного ИИ должны охраняться как объекты авторского права (рис. 5), и столько же полагают, что продукты генеративного ИИ должны охраняться правами интеллектуальной собственности (рис. 6).

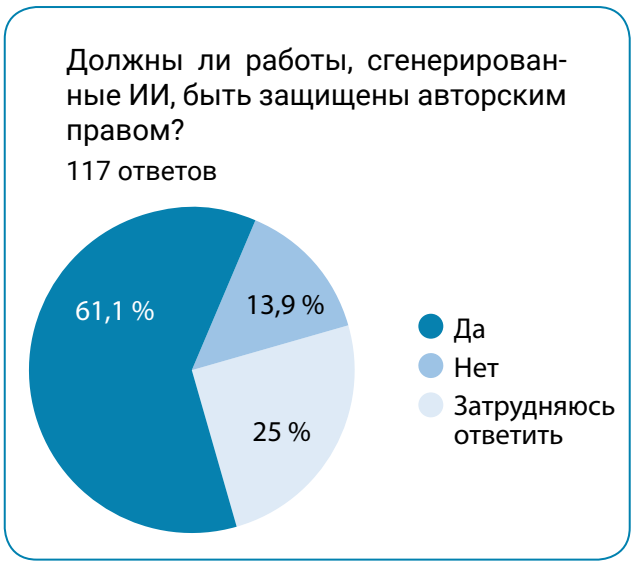


Рис. 5

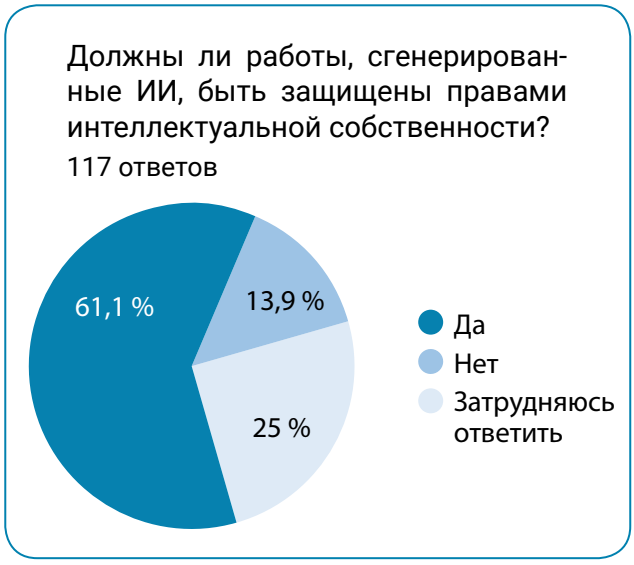


Рис. 6

Другой вопрос, на который еще предстоит ответить как создателям, так и потребителям: обладают ли созданные продукты художественной и культурной ценностью? И могут ли они на самом деле цениться так же высоко, как продукты творческого самовыражения человека? «*Это очень хороший вопрос. Для меня проблема заключается в том, что обычный человек скоро не сможет отличить одно от другого. Творческая деятельность зависит от личных предпочтений и мнений. Для меня сейчас гораздо важнее процесс создания произведения, добавление контекста и человеческого воображения при работе с ним, и умные авторы будут включать видеозаписи процесса создания произведения в качестве маркера подлинности для своей аудитории. Даже самый недобросовестный 'художник по запросам' не сможет этого сделать. А они, конечно, пытались*». Свое мнение высказывают и искусствоведы: некоторые из них сравнивают произведения искусства, созданные системами искусственного интеллекта, с произведениями, созданными обезьянами, поскольку и тем и другим не хватает «интенциональности» (Фадеева, 2023); другие считают смешение цифровых технологий и традиционного искусства новой реальностью (Степанов, 2022; Быльева, Краснощеков, 2023), а третьи утверждают, что использование таких технологий – не что иное, как очередной шаг к дегуманизации, и доказывают, что обычный человек не всегда понимает, какое произведение искусства создано человеком, а какое искусственным интеллектом (Пантелеев, 2023).

2.2. Плагиат, нарушение авторских прав и другие риски

Еще два вопроса, которые необходимо обсудить, – может ли генеративный ИИ вызвать недобросовестную конкуренцию и действительно ли представители индустрии считают, что производители и владельцы систем генеративного ИИ нарушают авторские права[37].

«Да, по обоим пунктам. Как свидетельствуют многочисленные иски и судебные разбирательства, поданные в этом году, разработчики этих платформ в той или иной степени знали о том, что их базы данных для ИИ содержат огромное количество материалов, защищенных авторским правом. Это острая, но тщательно избегаемая проблема. Без преувеличения, масштабы использования материалов, защищенных авторским правом, настолько велики и беспрецедентны, что представляют собой почти абстракцию; в некоторых случаях это затрудняет доказательство, но доказательства, безусловно, есть.

Другая сторона уравнения – компенсация. Творческих работников просто заменяют на ИИ. Примеров слишком много, чтобы их перечислять, но они оказывают существенное воздействие на творческую индустрию, которая традиционно недостаточно оплачивается и в значительной степени опирается на модель меценатства. Я всегда считал, что творческие работники – это, так сказать, канарейки в угольной шахте. Если ИИ не контролировать и не регулировать, то будут существенно затронуты многие отрасли.

Здесь следует отметить несколько моментов: во-первых, это популистское представление о том, что творческие люди – это луддиты, которые выступают против технологий. Я ни на секунду не верю в эту риторику. Проблема не в технологиях, а в злоупотреблении ими, как я уже отмечал ранее. Автоматизация на производстве, вероятно, необходима, поскольку повторяющиеся задачи в определенных условиях представляют опасность для жизни. Но этого нельзя сказать об автоматизации культуры, которую мы все считаем священной и которая, как и любой другой инструмент, может быть использована в неблаговидных целях. Таким образом, речь идет не только об авторском праве, но и о том, как технология влияет на нас в повседневной жизни».

Все вышесказанное подтверждается требованиями забастовок SAG-AFTRA[38] и WGA[39], Гильдии сценаристов[40], а также судебными исками против производителей генеративных систем искусственного интеллекта, такими как: 1) коллективный иск Sarah Andersen's, Kelly McKernan's and Karla Ortiz' class action vs. STABILITY AI LTD, Delaware corporation and DEVIANTART[41]; 2) иск Гильдии сценаристов против OpenAI Inc., где наиболее известная претензия состоит в том, что OpenAI даже не отрицает, что обучает свои системы на материалах, защищенных авторским правом[42].

С этим коррелирует и мнение англоязычных респондентов: 72,5 % из них согласны с тем, что производители генеративных систем ИИ нарушают авторские права, а 11,1 % с этим не согласны (рис. 7). Еще больше – 76,9 % респондентов – считают,

37 Case updates. Stable Diffusion litigation. (2023, October 31). https://clck.ru/36n4fM

38 We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

39 WGA Contract 2023. Summary of the 2023 WGA MBA. https://clck.ru/35shcD

40 Artificial Intelligence. The Authors Guild. https://clck.ru/36n4h8

41 United States District Court Northern District of California San Francisco Division. Stable Diffusion litigation. https://clck.ru/36n4hr

42 Authors Guild v. OpenAI Inc. (1:23-cv-08292). Court Listener. https://clck.ru/36n4mC

что такие компании нарушают права интеллектуальной собственности, однако 14,5 % высказывают противоположное мнение (рис. 8).

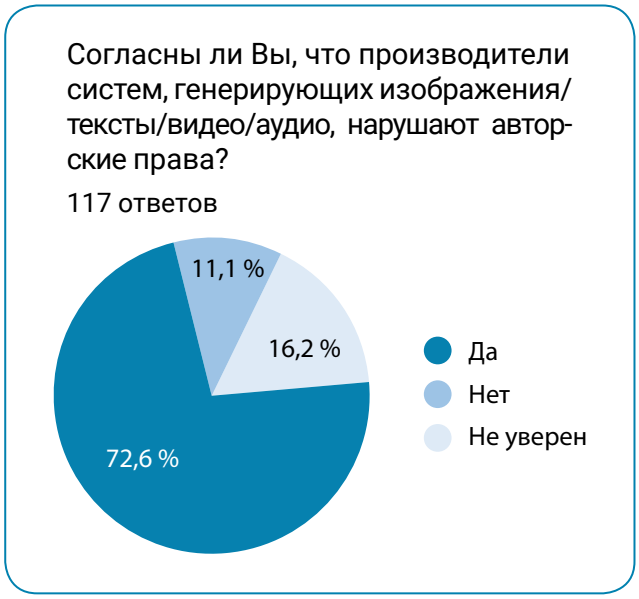


Рис. 7

Рис. 8

Русскоязычная аудитория продемонстрировала противоположную тенденцию – 50 % из нее не считают, что производители генеративных систем искусственного интеллекта нарушают авторские права (рис. 9), а 58,3 % не согласны с мнением о том, что такие компании нарушают права интеллектуальной собственности (рис. 10). Только 19,4 % русскоязычных респондентов разделяют точку зрения своих зарубежных коллег на нарушение авторских прав производителями генеративных систем искусственного интеллекта (рис. 9) и только 16,7 % поддерживают мнение о нарушении прав интеллектуальной собственности такими компаниями (рис. 10). В обоих случаях большая доля респондентов не уверена в своей позиции – 30,6 % (рис. 9) и 25 % (рис. 10) соответственно.

Рис. 9

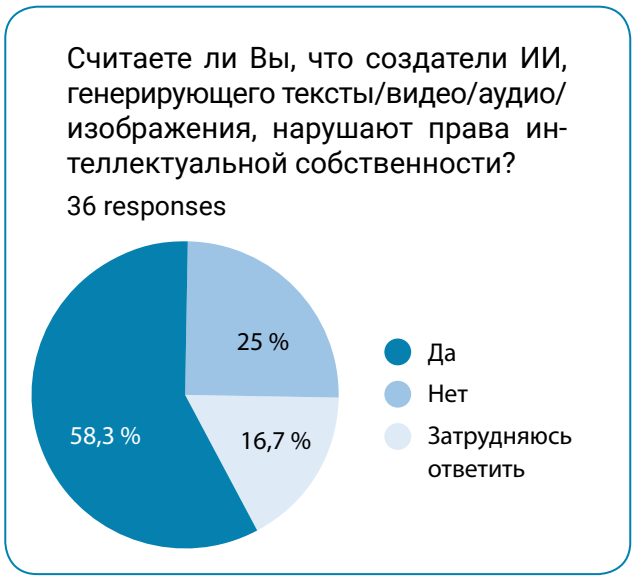


Рис. 10

Забастовка SAG-AFTRA ясно дала понять: участники считают искусственный интеллект экзистенциальной угрозой для своей профессии, поэтому лозунг «Мы боремся за выживание нашей профессии» означает, что благодаря генеративным системам искусственного интеллекта студии могут нанимать актера на один рабочий день, платить ему минимальную зарплату, но затем воспроизводить образ и голос этого актера, когда и как им вздумается[43]. Отсюда возникает другой вопрос: переживет ли творческая индустрия влияние такого массового использования генеративных систем искусственного интеллекта? Или это реальная угроза, которую нельзя игнорировать, пока не стало слишком поздно?

«В своей работе я видел, как люди берут хорошие деньги за то, чтобы быстро пропустить фотографии через фильтры искусственного интеллекта, и называют это готовым результатом. В попытке приспособиться к ситуации я обратился к совершенствованию процессов и контекстуализации работы как к основным генераторам ценности, поскольку именно это является подлинно человеческой деятельностью.

Сейчас угроза уже миновала, моя нишевая отрасль подготовлена. Однако, как гласит пословица, вы получаете то, за что платите. В моей конкретной области всегда будет существовать спрос на курирование, восстановление и контекстуализацию, осуществляемые человеком, и это привело к некоторым интересным разработкам в области получения дохода за счет использования своих сильных сторон, а не компенсации слабых. Генеративный ИИ просто не сможет повторить многие из тех процессов, которые мы наладили. Мы будем спокойно заниматься своими делами и оставим все как есть», – прокомментировал г-н Ллойд.

Мнения англоязычных респондентов несколько менее оптимистичны – 60,7 % считают, что генеративный ИИ представляет реальную угрозу для представителей творческой индустрии, 18,8 % с ними не согласны, 17,9 % не уверены, а 2,6 % утверждают, что их уже заменил генеративный ИИ (рис. 11).

В русскоязычной аудитории наблюдается прямо противоположная тенденция: 75 % респондентов не видят в генеративном ИИ угрозы для отрасли, 16,7 % видят такую угрозу, 8,3 % не уверены, и никто из респондентов не считает, что генеративный ИИ заменил его на рабочем месте (рис. 12).

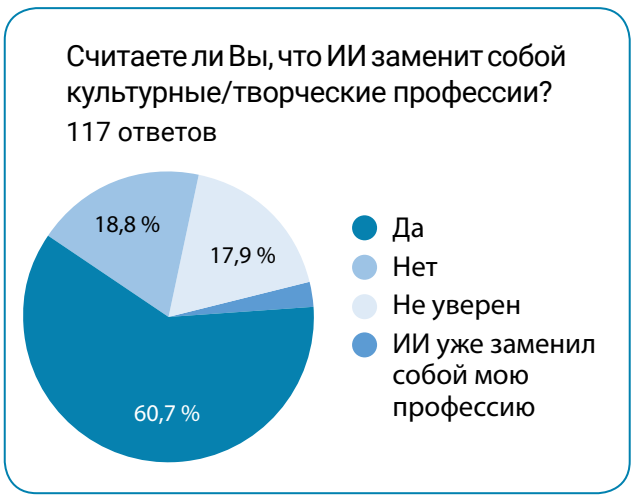


Рис. 11

Рис. 12

[43] We're Fighting for the Survival of Our Profession. SAG-AFTRA Strike. https://clck.ru/36n39G

Стоит отметить, что ответы русскоязычной аудитории коррелируют с общим взглядом российской креативной индустрии на эти технологии – в них склонны видеть только инструмент и философски комментировать, что инструменты не имеют души и, следовательно, не могут быть творцами, т. е. никогда не смогут заменить творцов-людей[44]. Но значит ли это, что использование генеративного ИИ в качестве инструмента в творческой индустрии может принести пользу? «*Прежде всего, важно различать некоторые понятия, которые сегодня смешиваются в дискуссиях об ИИ. В целом, являясь вспомогательным средством или инструментом в конкретной области приложения, ИИ делает возможным то, что раньше было невозможно, если брать конкретные рабочие процессы. В моей работе с архивными визуальными материалами – например, со сканами фотографий, – масштабирование до большего разрешения возможно только с использованием ИИ. Существуют и другие узкоспециализированные рабочие процессы, где применение ИИ в качестве инструмента или вспомогательного средства является просто частью более длительного технического процесса.*

Проблема возникает, когда пользователи путают идею 'помощи' или 'инструмента' с созданием нового материала, будь то картина в стиле реального художника или рассказ, сгенерированный по нескольким текстовым запросам. Такое 'генеративное' использование ИИ отличается от того, которое я описал выше. На мой взгляд, оно не является вспомогательным средством для создания производного или преобразующего произведения. На мой взгляд, здесь речь идет не о помощи в создании производного или трансформированного произведения, а лишь о подражании чему-то, уже созданному кем-то другим.

Другими словами, это разница между 'употреблением' и 'злоупотреблением'. Я много обсуждал использование генеративного искусственного интеллекта с творческими людьми. Я знаю одного художника, который использует Midjourney для того, чтобы сгенерировать несколько различных композиций с предметом, а затем выбирает одну из них в качестве визуального образца для полностью оригинальной работы, выполненной вручную. Я понимаю, что это экономит время для соблюдения сроков заказчика, и, на мой взгляд, это приемлемое использование технологии.

Также мне известна ситуация, когда автор самодеятельного издания выиграл приз за его обложку, а затем узнал, что художник получил большой гонорар за то, что собрал коллаж из нескольких рисунков, сгенерированных искусственным интеллектом. Сгенерированное изображение вряд ли можно считать производным или трансформированным произведением, поскольку в соответствии с законодательством Великобритании подобное произведение должно 'само по себе являться оригинальным произведением, созданным с использованием навыков, труда и суждений'. Кроме того, 'незначительные изменения, не меняющие существенно оригинал, не учитываются'.

В случае с художником обложки книги можно утверждать, что единственным творческим актом было окончательное расположение композиции созданных объектов. В случае с моим знакомым художником процесс создания был полностью делом рук и воображения человека.

Что касается генеративного ИИ, единственный возможный способ этичного использования, который я могу себе представить, – это если бы база данных содержала

[44] На «Горький fest» обсудили проблему участия нейросетей в кино. Bulleten Kinoprokatchika. https://clck.ru/36n4pf

только оригинальные работы, которые вы предоставили или взяли из фонда общественного достояния. К сожалению, как мы все знаем, это не так».

Все сказанное подтверждают и результаты расследований, проведенных Палатой общин в этом году. Участвовавшие в них эксперты выразили обеспокоенность по поводу злоупотреблений технологиями генеративного ИИ, которые становятся возможными из-за выявленных правовых пробелов и включают рост плагиата, замену людей-творцов генеративным ИИ и нарушения других прав. Однако при этом они предложили поощрять использование технологий ИИ (не только генеративных) в индустрии из-за их огромного потенциала, но только при условии, что такие технологии будут использоваться этично[45, 46].

В качестве еще одного примера злоупотребления генеративными технологиями ИИ можно привести недавний и довольно скандальный российский судебный процесс Алены Андроновой против банка «Тинькофф». Будучи актрисой дубляжа, она записала свой голос для нужд банка, но затем он был синтезирован и использован третьей стороной для дубляжа нескольких видов нелегального контента, в результате чего, как утверждается, она потеряла несколько контрактов[47].

С какими еще рисками сталкивается творческая индустрия в связи с массовым использованием технологий генеративного ИИ? «*Как уже отмечалось, недобросовестные лица просто хотят нажиться на небольшой, но постоянно вызывающей большой интерес у публики отрасли. Многие историки справедливо обеспокоены деконтекстуализацией исторического материала и отсутствием атрибуции. В этом отношении я с ними согласен. Я не совсем понимаю, каким может быть выход из сложившейся ситуации, но уверен, что отрасль достаточно мала, чтобы не впасть в коллапс из-за внедрения ИИ. Специалисты-практики должны осознавать свою этическую ответственность при выполнении своей работы*».

2.3. Маркировка продуктов генеративного ИИ

Анализируя китайский подход к правовому регулированию генеративного ИИ, можно сделать вывод, что маркировка ИИ рассматривается как мера защиты авторов и пользователей систем генеративного ИИ[48]. Недавно несколько компаний начали делать то же самое[49, 50] – наносить этикетки «создано с использованием ИИ», чтобы повысить прозрачность и способствовать ответственному использованию систем генеративного ИИ. По их утверждению, такое простое действие, как нанесение этикетки «создано с использованием ИИ», может предотвратить злоупотребление этими технологиями.

---

45 Connected tech: AI and creative technology: Eleventh Report of Session 2022–23. (2023). UK Parliament. https://clck.ru/36n3Sf

46 The governance of artificial intelligence: interim report. Ninth Report of Session 2022–23. (2023). UK Parliament. https://clck.ru/36n3TN

47 Информация по первичному документу № М-6609/2023. Oficialniy Portal Sudov Moskvy. https://clck.ru/36KzHu

48 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

49 AI Nutrition Facts. Twilio. https://clck.ru/36n4xc

50 Open Ethics Label: AI nutrition labels. Open Ethics. https://clck.ru/36n4yq

Как показывает мониторинг новостей, политики[51] и эксперты по цифровой безопасности[52] поддерживают эти заявления. Более того, они считают, что такая маркировка должна быть обязательной, поскольку в противном случае мы не сможем предотвратить постоянное распространение дезинформации и дипфейков. Это также крайне важно, учитывая тот факт, что правительство Великобритании уже связало их с такой опасной угрозой, как терроризм[53].

Но согласны ли представители отрасли с тем, что эта мера может быть настолько эффективной, как утверждают поставщики услуг[54, 55] по ИИ-маркировке? «*Я очень сомневаюсь в этом, хотя такое требование закона было бы крайне желательным. Как уже отмечалось выше, я сравниваю это с любой другой формой рекламы. Потребители должны знать, что то, что они видят или читают, создано искусственным интеллектом, и придерживаться тех же стандартов регулирования, что и рекламодатели со своей продукцией. В области 'ложной рекламы' действует хорошо отлаженный процесс регулирования. Снова и снова, когда маркетинговый отдел какой-либо компании обвиняют в использовании продуктов, созданных искусственным интеллектом, они сначала все отрицают, потом обычно недовольно соглашаются и делают заявление о необходимости скорректировать свои методы работы*».

В ответах на вопрос «Должны ли продукты генеративного ИИ быть помечены как таковые?» респонденты практически единодушно ответили утвердительно: 88 % англоязычных респондентов поддерживают эту идею и только 7,7 % считают ее излишней (рис. 13), а среди русскоязычных респондентов 80,6 % считают, что маркировка ИИ-продуктов должна быть обязательной, и только 13,9 % не одобряют эту идею (рис. 14).

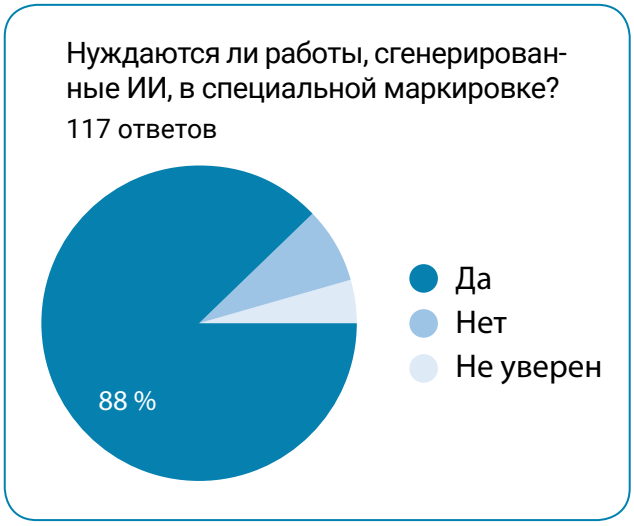


Рис. 13

Рис. 14

51 AI generated content should be labelled, EU Commissioner Jourova says. Reuters. https://clck.ru/36n5B8

52 Минцифры предложили ввести маркировку контента, созданного с помощью нейросетей. (2023, May 15). TASS. https://clck.ru/34RfkG

53 AI safety summit. Department For Science, Innovation and Technology. https://clck.ru/36n3zq

54 AI Nutrition Facts. Twilio. https://clck.ru/36n4xc

55 Open Ethics Label: AI nutrition labels. Open Ethics. https://clck.ru/36n4yq

Следует добавить, что технологически можно эффективно маркировать, или, как говорят другие исследователи, «ставить водяной знак» на всевозможные данные, включая цифровое аудио (Patil & Shelke, 2023), и даже делать это при необходимости незаметно (Liu et al., 2022). Кроме того, можно создать водяной знак, сохраняющийся на фотографиях (Cao et al., 2023). Различные методы нанесения водяных знаков могут помочь в аутентификации контента (Yuan et al., 2024), его защите и даже восстановлении (M. Swain & D. Swain, 2022). Однако другие исследования показывают, что водяной знак в нейронных сетях, например, не следует рассматривать как панацею, поскольку он может быть удален (Aiken et al., 2021).

2.4. Голос индустрии услышан

«*Интеллектуальная собственность, от научных исследований до художественного творчества, вносит большой вклад в экономику Великобритании. Как и во многих других странах, финансирование культуры и доступ к ней всегда представляли непростую задачу, и появление генеративного ИИ, безусловно, усугубит некоторые негативные аспекты этого процесса. Я считаю, что в интересах развития нашей законодательной базы необходимо как можно быстрее урегулировать эту проблему*».

Один из вопросов нашего исследования касался того, считают ли наши респонденты, что действующее законодательство их страны способно защитить их как профессионалов от негативного воздействия генеративного ИИ. Полученные данные подтверждают мнение о том, что неспособность государств адекватно и своевременно отвечать на запросы своих граждан является причиной политического недоверия населения к власти. Так, 72,6 % англоязычных респондентов не доверяют в этом вопросе действующим законодательным органам своих стран; 3,4 % считают, что их могут защитить существующие правовые нормы; 13,7 % не уверены, а 10,3 % являются потребителями продукции креативной индустрии, поэтому данный вопрос не предназначался для них (рис. 15).

Русскоязычная аудитория вновь демонстрирует более оптимистичный настрой, однако 50 % опрошенных не доверяют действующим в их странах законам о защите от генеративного ИИ, 16,7 % считают, что они уже достаточно защищены, а 33,3 % затруднились с ответом (рис. 16).

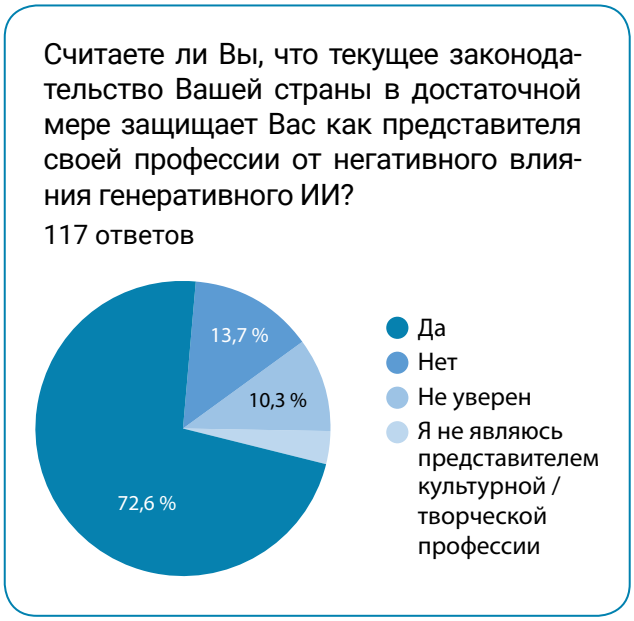


Рис. 15

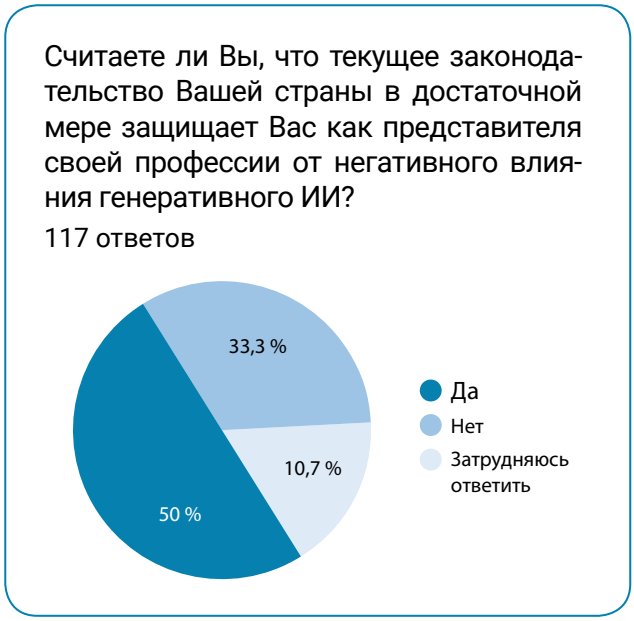


Рис. 16

И все же голос индустрии определенно не остался без внимания, по всему миру появляются многочисленные законодательные проекты, конечная цель которых – защитить как представителей творческой индустрии, так и потребителей ее продукции, а также повысить прозрачность и ответственность при использовании генеративных систем искусственного интеллекта.

Например, Гильдия сценаристов США (WGA) в сентябре прекратила свою забастовку – соглашение было достигнуто и ждет ратификации. Согласно ему: 1) ИИ не может писать или переписывать литературные произведения, а сгенерированный ИИ материал не будет считаться исходным материалом согласно Минимальному базовому соглашению, что означает, что сгенерированный ИИ материал не может быть использован для снижения оплаты или ущемления отдельных прав сценаристов; 2) сценарист может использовать ИИ при выполнении работы, если компания дает на это согласие и при условии, что сценарист следует применимым политикам компании, но компания не может требовать от сценариста использовать программное обеспечение ИИ (например, ChatGPT) при выполнении работ; 3) компания должна сообщить сценаристу, если какие-либо материалы, переданные ему, были полностью или частично сгенерированы искусственным интеллектом; 4) WGA оставляет за собой право утверждать, что использование материалов сценаристов для обучения искусственного интеллекта запрещено Минимальным базовым соглашением или другим актом[56].

Мнение Алены Андроновой также было услышано, несмотря на то, что суд оставил ее дело без движения[57]. После того как она совместно с Союзом дикторов и другими пострадавшими, чьи голоса «были украдены»[58], попыталась доказать, что человеческий голос является биометрической информацией, которую нельзя собирать без согласия лица, Совет Федерации принял решение о защите человеческого голоса от негативного воздействия генеративного ИИ и технологий глубокого синтеза и о мерах по предотвращению дальнейших правовых коллизий[59].

Сенат США также прислушался к представителям индустрии; он разработал аналогичный российскому законодательный акт, который в настоящее время известен как Закон против фейков и призван обеспечить правовую защиту «образа, голоса и визуального сходства» человека на весь период жизни и в течение 70 лет после смерти человека[60].

Европейский парламент, по-видимому, вдохновился китайским подходом[61] к регулированию генеративного ИИ, поскольку теперь он выдвигает следующие требования к производителям цифровых систем ИИ: 1) раскрывать информацию о том, что контент был сгенерирован искусственным интеллектом; 2) разрабатывать модель таким

---

56 WGA contract 2023. Summary of the 2023 WGA MBA. https://clck.ru/35shcD

57 Информация по первичному документу № М-6609/2023. Oficialniy Portal Sudov Moskvy. https://clck.ru/36KzHu

58 Andronova, A. (2023, August 30). Просим защитить наши голоса от воровства и мошенничества!. CHANGE ORG. https://clck.ru/36KzMK

59 В Совфеде предложили охранять голос человека и его синтез. PRAVO.RU. https://clck.ru/36j2Sy

60 Senate Legislative Counsel Draft Copy of EHF23968 GFW – To protect the image, voice, and visual likeness of individuals, and for other purposes. Senate GOV. https://clck.ru/36nut

61 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

образом, чтобы она не генерировала нелегальный контент; 3) публиковать сводки данных, защищенных авторским правом, которые использовались для обучения ИИ[62].

Кроме того, такие корпорации, как Microsoft[63], Adobe[64] и Google[65], приняли решение о защите пользователей своих генеративных систем искусственного интеллекта от исков, связанных с авторским правом и интеллектуальной собственностью, и даже пообещали выплачивать в таких случаях компенсацию. Microsoft поясняет, что новые меры также помогут представителям творческих профессий «сохранить контроль над своими правами в соответствии с законом об авторском праве и получать достойную прибыль от своих творений»[66].

Заключение

Проведенное исследование показало, что в настоящее время отсутствует универсальное понимание того, можно ли считать генеративный ИИ субъектом авторского права, а его продукты – объектами авторского права или прав на интеллектуальную собственность. Не существует также международной правовой базы, которая могла бы регулировать массовое использование таких технологий. Если такое регулирование не будет разработано в кратчайшие сроки, то неизбежен ущерб творческой индустрии, а через нее – экономике государств. Среди рисков, которые несет в себе нерегулируемое использование генеративных систем искусственного интеллекта, наш анализ выделил следующие: 1) нарушение авторских прав и прав интеллектуальной собственности; 2) нарушение моральных прав; 3) нарушение трудовых прав; 4) нарушение рынка труда; 5) нарушение прав потребителей; 6) массовое производство нелегального контента; 7) кризис оригинальности; 8) недобросовестная конкуренция; 9) недоверие общества к власти; 10) общественные беспорядки; 11) экстремизм и терроризм.

Для минимизации обозначенных рисков важно оперативно разработать новую международную и национальную правовую базу, которая позволит повысить подотчетность производителей, владельцев и пользователей систем генеративного ИИ и возложить на них ответственность за злоупотребление этими технологиями: «*Прежде всего, разработчики этих ИИ-сервисов должны быть открыты для контроля, не полагаться на техническую завуалированность и нести ответственность за свои обучающие данные. Ни у кого не возникло бы проблем, если бы разработчики просто придерживались принципов открытого доступа к материалам и участия по подписке. Во-вторых, необходимы более справедливые правила вознаграждения авторов, чьи работы попали в обучающие базы данных. Если у нас есть средства для массового сбора данных, то должны быть и средства для справедливого признания роли творческих работников и соответствующей оплаты их труда. В-третьих, коммерческое использование должно быть формализовано и регламентировано. Хорошим примером служит индустрия стоковой фотографии. Она процветает и хорошо себя зарекомендовала, при этом злоупотреблений этой системой сравнительно немного, что коммерчески обосновано и выгодно как*

62 EU AI Act: first regulation on artificial intelligence. EU Parlaiment. https://clck.ru/36n5Lv

63 Microsoft announces new Copilot Copyright Commitment for customers. Microsoft. https://clck.ru/36n5MQ

64 Adobe offers copyright indemnification for Firefly AI-based image app users. Computer World. https://clck.ru/36n5Mx

65 Shared fate: Protecting customers with generative AI indemnification. Google. https://clck.ru/36n5NP

66 Microsoft announces new Copilot Copyright Commitment for customers. Microsoft. https://clck.ru/36n5MQ

владельцам платформ, так и творческим работникам, которые предоставляют им свои работы. Я не вижу причин, по которым не может быть реализовано соглашение о подписке на использование генеративного искусственного интеллекта в той или иной форме, чтобы остановить безудержное злоупотребление им. В-четвертых, необходимо особенно бдительно следить за тем, как поисковые системы представляют материалы, созданные искусственным интеллектом. Как это достигается на техническом уровне, я сказать не берусь, но, повторюсь, это возможно».

Можно также констатировать, что в странах с различными режимами начали приниматься более или менее схожие меры, близкие к тем, что применяются в Китае[67], которые включают: 1) прозрачность данных, используемых для обучения; 2) маркировку продуктов генеративных систем ИИ; 3) ответственность за нарушение авторских прав и прав интеллектуальной собственности; 4) защиту образа, голоса и визуального сходства человека. По нашему мнению, в обозримом будущем использование генеративных систем ИИ будет регулироваться аналогичными мерами и на международном уровне.

В заключение хотелось бы подчеркнуть, что вопрос этичности использования генеративного ИИ выходит далеко за рамки вопроса «кто автор?» и затрагивает не только творческую индустрию. Он также оказывает влияние на экономику государств и даже на сами демократические институты, что, как показал наш анализ, обусловливает необходимость восполнения существующих правовых пробелов, включая такую простую, на первый взгляд, проблему, как отсутствие соответствующей терминологии.

Список литературы

Агибалова, Е. Н., Перекрёстова, Е. А. (2020). Право авторства на произведения, созданные искусственным интеллектом. *Эпоха науки*, *24*, 124–126. https://doi.org/10.24411/2409-3203-2020-12424

Быльева, Д. С., Краснощеков, В. В. (2023). Оригинал и копия: технологический вызов искусству. *Вестник Московского государственного областного университета. Серия: Философские науки*, 2, 77–91. https://doi.org/10.18384/2310-7227-2023-2-77-91

Пантелеев, А. Ф. (2023). Проблема сравнительной оценки картин, созданных художником и сгенерированных нейросетью. *Известия Саратовского университета. Новая серия. Серия: Философия. Психология. Педагогика*, *23*(3), 326–330. https://doi.org/10.18500/1819-7671-2023-23-3-326-330

Соменков, С. А. (2019). Искусственный интеллект: от объекта к субъекту? *Вестник Университета имени О. Е. Кутафина*, *2*(54), 75–85. https://doi.org/10.17803/2311-5998.2019.54.2.075-085

Степанов, М. А. (2022). Деавтономия постчеловеческого воображения: новые направления в теории искусства. В сб: *Актуальные проблемы теории и истории искусства* (№ 12, с. 663–673). http://dx.doi.org/10.18688/aa2212-07-53

Фадеева, Т. Е. (2023). «Союз» художника с нечеловеческим агентом – утопия или рабочая модель художественного производства? *Известия Самарского научного центра Российской академии наук. Социальные, гуманитарные, медико-биологические науки*, *25*, 1(88), 108–115. https://doi.org/10.37313/2413-9645-2023-25-88-108-115

Aiken, W., Kim, H., Woo, S. S., & Ryoo, J. (2021). Neural network laundering: Removing black-box backdoor watermarks from deep neural networks. *Computers & Security*, *106*, 102277. https://doi.org/10.1016/j.cose.2021.102277

Cao, F., Wang, T., Guo, D., Li, J., & Qin, C. (2023). Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain. *Journal of Visual Communication and Image Representation*, *94*, 103837. https://doi.org/10.1016/j.jvcir.2023.103837

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023).

[67] 生成式人工智能服务管理暂行办法. 1994. No. 143. 国家互联网信息办公室. (2023). 第15号. https://goo.su/fbbG

Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Fenwick, M., & Jurčys, P. (2023). Originality and the future of copyright in an age of generative AI. *Computer Law & Security Review*, 105892. https://doi.org/10.1016/j.clsr.2023.105892

Küçükkömürler, S., & Özkan, T. (2022). Political interest across cultures: The role of uncertainty avoidance and trust. *International Journal of Intercultural Relations*, *91*, 88–96. https://doi.org/10.1016/j.ijintrel.2022.09.004

Liu, G., Xiang, R., Liu, J., Pan, R., & Zhang, Z. (2022). An invisible and robust watermarking scheme using convolutional neural networks. *Expert Systems With Applications*, *210*, 118529. https://doi.org/10.1016/j.eswa.2022.118529

Patil, A. P., & Shelke, R. (2023). An effective digital audio watermarking using a deep convolutional neural network with a search location optimization algorithm for improvement in Robustness and Impercepetibility. *High-Confidence Computing*, 100153. https://doi.org/10.1016/j.hcc.2023.100153

Sparkes, M. (2022). AI copyright. *New Scientist*, *256*(3407), 17. https://doi.org/10.1016/s0262-4079(22)01807-3

Stokel-Walker, C. (2023). ChatGPT's knowledge of copyrighted novels highlights legal uncertainty of AI. *New Scientist*, *258*(3438), 13. https://doi.org/10.1016/s0262-4079(23)00837-0

Stroppe, A. (2023). Left behind in a public services wasteland? On the accessibility of public services and political trust. *Political Geography*, *105*, 102905. https://doi.org/10.1016/j.polgeo.2023.102905

Swain, M., & Swain, D. (2022). An effective watermarking technique using BTC and SVD for image authentication and quality recovery. *Integration*, *83*, 12–23. https://doi.org/10.1016/j.vlsi.2021.11.004

Torres, G. & Bellinger, N. (2014). The Public Trust: The Law's DNA. *Cornell Law Faculty Publications*. Paper 1213. http://scholarship.law.cornell.edu/facpub/1213

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, *42*, 105581. https://doi.org/10.1016/j.clsr.2021.105581

Yuan, Z., Zhang, X., Wang, Z., & Yin, Z. (2024). Semi-fragile neural network watermarking for content authentication and tampering localization. *Expert Systems With Applications*, *236*, 121315. https://doi.org/10.1016/j.eswa.2023.121315

Информация об авторах

Шумакова Наталья Игоревна – доцент кафедры конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Российская Федерация, г. Челябинск, пр. Ленина, 76
E-mail: shumakovani@susu.ru
ORCID ID: http://orcid.org/0009-0004-6053-0650
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

Ллойд Джордан Дж. – Шеффилдский университет; креативный директор, компания «Unseen History»
Адрес: Хоуес Фарм, Доддингхерст Роуд, Брентвуд, Эссекс, CM15 0SG, Великобритания
E-mail: jordan@unseenhistories.com
ORCID ID: https://orcid.org/0009-0007-8733-7261

Титова Елена Викторовна – доктор юридических наук, доцент, директор Юридического института, заведующий кафедрой конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Российская Федерация, г. Челябинск, пр. Ленина, 76
E-mail: titovaev@susu.ru
ORCID ID: http://orcid.org/0000-0001-9453-3550
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201640405
Google Scholar ID: https://scholar.google.ru/citations?user=Pqj6OiQAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=451302

Вклад авторов

Идея статьи является совместной и принадлежит Н. И. Шумаковой и Дж. Дж. Ллойду.
Н. И. Шумакова осуществляла формулирование идеи; выполняла составление черновика и чистовика рукописи; разработала дизайн методологии; организовала проведение социологических опросов; осуществляла сбор и анализ литературы и законодательства; сформулировала ключевые выводы, предложения и рекомендации.
Дж. Дж. Ллойд составил, обработал и предоставил свое экспертное мнение по ключевым положениям статьи; провел выборку публикаций в медиа; осуществлял интерпретацию общих результатов исследования.
Е. В. Титова осуществляла анализ законодательства; рассмотрела с точки зрения проявления публичного/политического недоверия процессы, происходящие в творческой индустрии; провела частичный сбор и анализ научной литературы.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Авторы выражают благодарность редакции Journal of Digital Technologies and Law за помощь в проведении социологического опроса в телеграм-канале журнала https://t.me/JournalDTL

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.41.91 / Авторское право и смежные права в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 31 октября 2023 г.
Дата одобрения после рецензирования – 20 ноября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.38

Towards Legal Regulations of Generative AI in the Creative Industry

Natalia I. Shumakova ✉

Law Institute, South Ural State University (national research university)
Chelyabinsk, Russia

Jordan J. Lloyd

Unseen History
Essex, United Kingdom

Elena V. Titova

Law Institute, South Ural State University (national research university)
Chelyabinsk, Russia

Keywords

artificial intelligence,
copyright law,
creative industry,
digital technologies,
generative artificial intelligence,
intellectual property,
international law,
neural network,
object of copyright law,
subject of copyright law

Abstract

Objective: this article aims to answer the following questions: 1. Can generative artificial intelligence be a subject of copyright law? 2. What risks the unregulated use of generative artificial intelligence systems can cause? 3. What legal gaps should be filled in to minimize such risks?

Methods: comparative legal analysis, sociological method, concrete sociological method, quantitative data analysis, qualitative data analysis, statistical analysis, case study, induction, deduction.

Results: the authors identified several risks of the unregulated usage of generative artificial intelligence in the creative industry, among which are: violation of copyright and labor law, violation of consumers rights and the rise of public distrust in government. They suggest that a prompt development of new legal norms can minimize these risks. In conclusion, the article constants that states have already begun to realize that the negative impact of generative artificial intelligence on the creative industry must not be ignored, hence the development of similar legal regulations in states with completely different regimes.

✉ Corresponding author

Scientific novelty: the article provides a comprehensive study of the impact of generative artificial intelligence on the creative industry from two perspectives: the perspective of law and the perspective of the industry. The empirical basis of it consists of two international surveys and an expert opinion of a representative of the industry. This approach allowed the authors to improve the objectivity of their research and to obtain results that can be used for finding a practical solution for the identified risks. The problem of the ongoing development and popularization of generative artificial intelligence systems goes beyond the question "who is the author?" therefore, it needs to be solved by introduction of other than the already existing mechanisms and regulations – this point of view is supported not only by the results of the surveys but also by the analysis of current lawsuits against developers of generative artificial intelligence systems.

Practical significance: the obtained results can be used to fasten the development of universal legal rules, regulations, instruments and standards, the current lack of which poses a threat not only to human rights, but also to several sectors within the creative industry and beyond.

For citation

Shumakova, N. I., Lloyd, J. J., & Titova, E. V. (2023). Towards Legal Regulations of Generative AI in the Creative Industry. *Journal of Digital Technologies and Law, 1*(4), 880–908. https://doi.org/10.21202/jdtl.2023.38

References

Agibalova, E. N., & Perekrestova, E. A. (2020). Copyright for the works created by artificial intelligence. *Ehpokha nauki*, *24*, 124–126. (In Russ.). https://doi.org/10.24411/2409-3203-2020-12424

Aiken, W., Kim, H., Woo, S. S., & Ryoo, J. (2021). Neural network laundering: Removing black-box backdoor watermarks from deep neural networks. *Computers & Security*, *106*, 102277. https://doi.org/10.1016/j.cose.2021.102277

Bylieva, D., & Krasnoschekov, V. (2023). The original and a copy: a technological challenge to art. *Bulletin of the Moscow Region State University*. Series: Philosophy, 2, 77–91. (In Russ.). https://doi.org/10.18384/2310-7227-2023-2-77-91

Cao, F., Wang, T., Guo, D., Li, J., & Qin, C. (2023). Screen-shooting resistant image watermarking based on lightweight neural network in frequency domain. *Journal of Visual Communication and Image Representation*, *94*, 103837. https://doi.org/10.1016/j.jvcir.2023.103837

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M. L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Fadeeva, T. E. (2023). "Union" of an artist with a non-human agent: utopia or a working model of artistic production? Izvestiya of the Samara Science Centre of the Russian Academy of Sciences. *Social, Humanitarian, Biomedical Sciences*, *25*(88), 108–115. (In Russ.). https://doi.org/10.37313/2413-9645-2023-25-88-108-115

Fenwick, M., & Jurčys, P. (2023). Originality and the future of copyright in an age of generative AI. *Computer Law & Security Review*, 105892. https://doi.org/10.1016/j.clsr.2023.105892

Küçükkömürler, S., & Özkan, T. (2022). Political interest across cultures: The role of uncertainty avoidance and trust. *International Journal of Intercultural Relations*, *91*, 88–96. https://doi.org/10.1016/j.ijintrel.2022.09.004

Liu, G., Xiang, R., Liu, J., Pan, R., & Zhang, Z. (2022). An invisible and robust watermarking scheme using convolutional neural networks. *Expert Systems With Applications*, *210*, 118529. https://doi.org/10.1016/j.eswa.2022.118529

Panteleev, A. F. (2023). The problem of comparative evaluation of paintings created by an artist and generated by a neural network. Izvestiya of Saratov University. *Philosophy. Psychology. Pedagogy*, *23*(3), 326–330. (In Russ.). https://doi.org/10.18500/1819-7671-2023-23-3-326-330

Patil, A. P., & Shelke, R. (2023). An effective digital audio watermarking using a deep convolutional neural network with a search location optimization algorithm for improvement in Robustness and Impercepetibility. *High-Confidence Computing*, 100153. https://doi.org/10.1016/j.hcc.2023.100153

Somenkov, S. A. (2019). Artificial intelligence: from object to subject? *Courier of the Kutafin Moscow State Law University*, *2*(54), 75–85. (In Russ.). https://doi.org/10.17803/2311-5998.2019.54.2.075-085

Sparkes, M. (2022). AI copyright. *New Scientist*, *256*(3407), 17. https://doi.org/10.1016/s0262-4079(22)01807-3

Stepanov, M. A. (2022). De-Autonomy of Post-Human Imagination: New Directions in the Theory of Art. *Actual Problems of Theory and History of Art* (No.*12*, pp. 663–673). (In Russ.). http://dx.doi.org/10.18688/aa2212-07-53

Stokel-Walker, C. (2023). ChatGPT's knowledge of copyrighted novels highlights legal uncertainty of AI. *New Scientist*, *258*(3438), 13. https://doi.org/10.1016/s0262-4079(23)00837-0

Stroppe, A. (2023). Left behind in a public services wasteland? On the accessibility of public services and political trust. *Political Geography*, *105*, 102905. https://doi.org/10.1016/j.polgeo.2023.102905

Swain, M., & Swain, D. (2022). An effective watermarking technique using BTC and SVD for image authentication and quality recovery. *Integration*, *83*, 12–23. https://doi.org/10.1016/j.vlsi.2021.11.004

Torres, G. & Bellinger, N. (2014). The Public Trust: The Law's DNA. *Cornell Law Faculty Publications*. Paper 1213. http://scholarship.law.cornell.edu/facpub/1213

Wan, Y., & Lu, H. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, *42*, 105581. https://doi.org/10.1016/j.clsr.2021.105581

Yuan, Z., Zhang, X., Wang, Z., & Yin, Z. (2024). Semi-fragile neural network watermarking for content authentication and tampering localization. *Expert Systems With Applications*, *236*, 121315. https://doi.org/10.1016/j.eswa.2023.121315

Authors information

Natalia I. Shumakova – Associate professor of law, Department of constitutional and administrative law, Law Institute, South Ural State University (national research university), Chelyabinsk, Russia
Address: 76 Lenin Str., 454080 Chelyabinsk, Russian Federation
E-mail: shumakovani@susu.ru
ORCID ID: http://orcid.org/0009-0004-6053-0650
RSCI Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

Jordan J. Lloyd – Creative Director, Unseen History
Address: Howes Farm, Doddinghurst Road, Brentwood, Essex, CM15 0SG, United Kingdom
E-mail: jordan@unseenhistories.com
ORCID ID: https://orcid.org/0009-0007-8733-7261

Elena V. Titova – Dr. Sci. (Law), Associate Professor, Department of Constitutional and Administrative Law, Law Institute, South Ural State University (National Research University)
Address: 76 Lenin Str., 454080 Chelyabinsk, Russian Federation
E-mail: titovaev@susu.ru
ORCID ID: http://orcid.org/0000-0001-9453-3550
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57201640405
Google Scholar ID: https://scholar.google.ru/citations?user=Pqj6OiQAAAAJ
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=451302

Authors' contributions

The idea of the article is joint and belongs to Natalia I. Shumakova and Jordan J. Lloyd.
Natalia I. Shumakova formulated the idea; drafted the manuscript; developed the methodology; organized sociological surveys; collected and analyzed literature and legislation; formulated key conclusions, proposals and recommendations.
Jordan J. Lloyd drafted, processed and presented his expert opinion on the key provisions of the article; sampled media publications; interpreted the overall results of the study.
Elena V. Titova analyzed legislation; considered the processes occurring in the creative industry from the viewpoint of public/political distrust manifestation; partially collected and analyzed scientific literature.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The authors are grateful to the Editorial Office of the Journal of Digital Technologies and Law for their assistance in conducting a sociological survey in the Journal's Telegram channel at https://t.me/JournalDTL

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – October 31, 2023
Date of approval – November 20, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:34.096:347.211:004.8
EDN: https://elibrary.ru/phbnki
DOI: https://doi.org/10.21202/jdtl.2023.39

Авторские права на результаты деятельности искусственного интеллекта и способы их защиты

Дмитрий Александрович Казанцев

B2B-Center
г. Москва, Российская Федерация

Ключевые слова

деликтоспособность,
интеллектуальная собственность,
искусственный интеллект,
нейросеть,
право,
правоспособность,
правосубъектность,
робот,
творчество,
цифровые технологии

Аннотация

Цель: обоснование механизмов правовой защиты объектов интеллектуальной собственности, созданных с использованием искусственного интеллекта.

Методы: использование искусственного интеллекта для создания произведений, традиционно относящихся к объектам авторского права, исследовалось посредством совокупности общенаучных и теоретико-правовых методов научного познания, включая сравнение, аналогию и синтез. Кроме того, практика использования искусственного интеллекта, в том числе нейросетей, для создания таких произведений была рассмотрена в нескольких аспектах на основе ретроспективного и многофакторного анализа.

Результаты: в работе обобщена актуальная практика использования искусственного интеллекта для создания произведений, традиционно относящихся к объектам интеллектуальной собственности (текстов, изображений, музыки, программ для ЭВМ), с учетом сформулированных научных и правовых позиций. Выделено несколько качественно различающихся между собой вариантов использования искусственного интеллекта. Для каждого из этих вариантов был предложен механизм правовой защиты, а также указаны области эффективного их применения. Даны предложения по регулированию правовой защиты результатов деятельности искусственного интеллекта не в парадигме конкурирующих доктрин, а в сочетании нескольких инструментов с применением каждого из них в релевантной ситуации.

Научная новизна: в работе представлена онтологическая дифференциация результатов деятельности искусственного интеллекта и соответствующих им механизмов правовой защиты. Созданные искусственным интеллектом результаты деятельности предлагается считать не единым объектом правового регулирования, а совокупностью внешне сходных, но онтологически различных объектов, каждый из которых требует собственного подхода к правовой охране.

Практическая значимость: предложенная в настоящей работе онтологическая дифференциация результатов деятельности искусственного интеллекта и соответствующих им механизмов правовой защиты актуальна как в качестве основы для дальнейших исследований, так и в качестве предложений для дополнения норм гражданского законодательства.

Для цитирования

Казанцев, Д. (2023). Авторские права на результаты деятельности искусственного интеллекта и способы их защиты. *Journal of Digital Technologies and Law*, *1*(4), 909–931. https://doi.org/10.21202/jdtl.2023.39

Содержание

Введение

Цифровые технологии – это важный фактор настоящего и ключевая компонента будущего. Сегодня уместно говорить не просто об экспериментах по внедрению искусственного интеллекта и алгоритмов обработки больших данных, а о консенсусе по вопросу о необходимости подобных инноваций. В Стратегии развития информационного общества, утвержденной Указом Президента Российской Федерации № 203 от 9 мая 2017 г., особо отмечается, что конкурентным преимуществом на мировом рынке обладают те государства, отрасли экономики которых основываются на технологиях анализа больших объемов данных[1]. И с этим тезисом сложно поспорить: хозяйственная практика с каждым годом все яснее демонстрирует конкурентные преимущества роботизации и использования искусственного интеллекта.

Распространение цифровых технологий в целом и практик использования искусственного интеллекта в частности преобразовывает в том числе и творческую реальность. Различные технологии, основанные на обработке больших данных

[1] Указ Президента Российской Федерации № 203 от 09.05.2017. (2017). Собрание законодательства Российской Федерации, 20, ст. 2901.

и машинном самообучении, перешли из области экспериментов в область хозяйственного и даже бытового применения. Проще говоря, с помощью искусственного интеллекта любой человек, обладающий базовыми знаниями об информационных технологиях, может не только получать информацию, но и создавать ее.

Такие объекты, как текст, изображение и музыкальное произведение, традиционно относятся к объектам интеллектуальной собственности. Однако сегодня они создаются с использованием искусственного интеллекта. Это означает, что не только в отвлеченном философском дискурсе, но и в прикладном правовом смысле становятся актуальными следующие вопросы:

1. Является ли произведение, созданное искусственным интеллектом, результатом творческой деятельности?

2. Является ли такое произведение объектом авторских прав?

3. Является ли такое произведение объектом интеллектуальной собственности?

Эти вопросы связаны между собой, однако каждый из них характеризует обособленный феномен правового порядка. Их актуальность обуславливается не только инновационным характером технологий, подлежащих анализу для корректного ответа на данные вопросы, но и повсеместным распространением таких технологий.

Так, мы должны уяснить себе, позволяют ли сегодняшние технологии признавать за искусственным интеллектом правовую субъектность. Смежным, но при этом отдельным вопросом является проблема признания искусственного интеллекта автором произведения. Сочетание этих фундаментальных правовых позиций с ответами на означенные выше вопросы и создает основу для правового регулирования результатов деятельности искусственного интеллекта, которое уже сегодня является не только возможным, но и необходимым. При этом важно помнить о том, что надлежащее и эффективное регулирование возможно лишь в том случае, когда регулирующие нормы адекватно отражают суть регулируемых объектов.

А потому для симметричного ответа на вопрос о возможности авторского права на результаты деятельности искусственного интеллекта необходимо проанализировать сущность самой такой деятельности. В принципе, данная тема не может быть полностью раскрыта исключительно в правовом поле и требует междисциплинарного подхода. И хотя в рамках статьи рассматривается лишь регуляторная грань проблемы, но при формулировке правовых позиций не обойтись без ссылок, по крайней мере, на базовые технологические аспекты и принципы работы искусственного интеллекта.

Последовательные ответы на предложенные выше вопросы должны учитывать отсутствие в научном сообществе консенсуса как по вопросу о сущности когнитивной деятельности искусственного интеллекта, так и по вопросу о его правосубъектности.

Сразу стоит оговориться, что за рамками данной статьи остаются такие вопросы, связанные с правосубъектностью искусственного интеллекта, как статус робота-водителя и порядок распределения и реализации юридической ответственности за причиненный им вред. Этим вопросам посвящены специальные исследования, которые в основном склоняются к выводу о субсидиарной ответственности (Duffy & Hopkins, 2017), а точнее, о матрице ответственности, на основании которой вопрос о возложении неблагоприятных правовых последствий решается индивидуально в каждом конкретном случае с учетом комплекса фактов (Colonna, 2012).

Упоминание автоматизированного вождения возвращает нас к более общему вопросу об ответственности за вред, ставший следствием работы искусственного

интеллекта (Bertolini, 2013). На сегодня вопрос о деликтоспособности искусственного интеллекта представляется актуальным более в практической, нежели в правовой плоскости, поскольку пока что умышленная или по меньшей мере неосторожная вина «посредников искусственного интеллекта (разработчиков и пользователей) в случае нанесения вреда системой искусственного интеллекта может быть вполне вероятной, юридически и экспертно доказуемой» (Bertolini, 2013).

Вопросом еще более высокого порядка является вопрос о том, кто становится стороной не только в деликтном, но и в любом правоотношении, порожденном действиями искусственного интеллекта. Например, если последствиями действий искусственного интеллекта стало правовое бытие нового договора, то кто именно будет считаться сторонами такого договора?

И вот этот-то уровень обобщения подводит нас к вопросу, непосредственно касающемуся темы данной статьи. Обладает ли робот правовой субъектностью? Вопрос об авторских правах на результаты деятельности искусственного интеллекта не сводится к вопросу о правовой субъектности, однако непосредственно связан с ним.

1. Робот как субъект права

Если мы признаем искусственный интеллект в качестве субъекта права в целом, то из этого признания логично следует положительное решение таких вопросов, как наличие у него авторского права и иных прав интеллектуальной собственности на созданные им произведения.

Однако можно ли рассматривать искусственный интеллект реально – или, по крайней мере, потенциально – в качестве правового субъекта с органически присущими ему правами и обязанностями? Ответ на этот вопрос не так-то прост.

Например, Резолюция Европейского парламента от 16 февраля 2017 г. с рекомендациями Комиссии по гражданскому праву «Правила робототехники», указывая на возрастающую актуальность вопроса об ответственности за вред, причиненный искусственным интеллектом, отмечает вместе с тем, что действующее законодательство не позволяет привлечь искусственный интеллект даже в случае, когда наносят ущерб третьим лицам[2]. И хотя в данной Резолюции перспективы правовой субъектности искусственного интеллекта описаны с подчеркнутой осторожностью, но в проекте от 31 мая 2016 г. были сформулированы несколько подходов к закреплению «правовой природы искусственного интеллекта: рассматривать как физических лиц, как юридические лица, как животных или объекты либо создать новую категорию, с ее собственными особенностями и последствиями в отношении присвоения прав и обязанностей, включая ответственность за ущерб»[3].

Со времени принятия резолюции вопрос о правовой субъектности искусственного интеллекта не теряет своей актуальности, а дебаты по этому вопросу интенсифицируются с каждым годом. Несколько упрощая, в международной дискуссии можно выделить несколько ключевых подходов к решению этого вопроса: констатация

---

2 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

3 Committee on Legal Affairs. (2016, May 31). Draft report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). https://clck.ru/36hAPJ

отсутствия возможности признания правосубъектности за искусственным интеллектом (Calo et al., 2018), применение юридической фикции с установлением для искусственного интеллекта правосубъектности, подобной правосубъектности юридических лиц (Solaiman, 2017), или даже формирование новой отрасли законодательства, посвященной специфическому регулированию статуса искусственного интеллекта и релевантной этой специфики (Cofone, 2018).

Заслуживает внимания мнение видных российских исследователей о том, что сегодня «наиболее рациональным, но не бесспорным видится использование концепции правосубъектности искусственного интеллекта по типу юридического лица либо электронного лица; подход к правовому регулированию в рамках юридической ответственности, связанной с пользователями, владельцами или производителями систем искусственного интеллекта, а не с технологическими объектами» (Ивлиев, Егорова, 2022). Концепцию «электронного лица» как нового субъекта права стоит вспомнить при обсуждении вопроса об интеллектуальных правах на результаты деятельности искусственного интеллекта. Здесь же стоит отметить то, что правосубъектность искусственного интеллекта может иметь черты сходства с правосубъектностью юридического лица, однако по целому ряду причин не может быть тождественна ей.

Сразу необходимо оговориться, что вопрос правовой субъектности искусственного интеллекта невозможно решать раз и навсегда. «То, что составляет ‘искусственный интеллект’, субъективно и лучше всего описывается как движущаяся мишень. То, что является искусственным интеллектом для одного человека, не обязательно является им для другого; то, что считалось искусственным интеллектом, скажем, пятнадцать лет назад, сегодня считается обычным явлением; даже вопрос ‘что такое интеллект?’ вызывает споры» (Greenstein, 2022).

Статус искусственного интеллекта в правовых отношениях во многом зависит как от достигнутого уровня развития техники, позволяющего роботу выполнять определенные мыслительные функции, так и от уровня развития общественных отношений, в которых деятельность искусственного интеллекта может иметь более или менее существенное значение. И с точки зрения достигнутого уровня развития техники на сегодняшний день «очевидна несостоятельность предложения признания за искусственным интеллектом правосубъектности, аналогичной правосубъектности физического лица, и, несмотря на использование принципов работы человеческого мозга для построения системы искусственного интеллекта, принципы правового регулирования статуса физического лица не могут быть применены к искусственному интеллекту» (Дурнева, 2019).

Ведь способность порождать правоотношения – это лишь часть правосубъектности. Полноценный правовой субъект осуществляет права и несет обязанности, а также при наличии соответствующих оснований несет ответственность. Возможность реального применения мер той же ответственности к искусственному интеллекту сегодня вызывает большие сомнения. Не говоря уже о том, что категория вины – будь то умысел или неосторожность – и вовсе не соотносится с феноменом искусственного интеллекта.

Более того, наделение искусственного интеллекта в нынешнем его виде правовой субъектностью содержит в себе потенциальную угрозу верховенству права. Ведь правосубъектность включает в себя и способность принимать юридически значимые решения. «Угроза верховенству закона заключается в том, что большинство

таких систем принятия решений являются ‘черными ящиками’, поскольку в них заложены чрезвычайно сложные технологии, которые, по сути, находятся за пределами когнитивных возможностей человека, и закон тоже в определенной степени препятствует прозрачности. При этом оказываются практически невыполнимыми такие требования верховенства права, как понятность, прозрачность, справедливость и объяснимость, что, в свою очередь, ставит вопрос о том, насколько верховенство права является жизнеспособной концепцией в технократическом обществе» (Greenstein, 2022).

И это, в свою очередь, подводит нас к аспекту, важному для решения вопроса об авторстве искусственного интеллекта. Не является ли механистическое перенесение на искусственный интеллект категорий, присущих человеческому сознанию, будь то категория вины или категория творчества, необоснованным приданием роботу антропоморфных черт? И речь здесь вовсе не о пресловутом «эффекте зловещей долины», а о куда более фундаментальных, онтологических аспектах.

Необходимо со всей ясностью осознавать то, что дискуссию о правах роботов мы в любом случае ведем с антропоцентрической точки зрения. Это касается и аксиологического измерения, в которым мы признаем правом и ценностью именно то, что кажется правом и ценностью нам, людям, притом что юриспруденция совсем не случайно именуется именно социально-гуманитарной, а отнюдь не естественной наукой. Это же касается и утилитарной точки зрения.

Проще говоря, в конечном счете мы хотим наделить роботов правосубъектностью для того, чтобы они могли отвечать за свои действия перед нами, людьми.

В уже упомянутой выше Резолюции Европарламента эта мысль сформулирована обтекаемо и несколько двусмысленно: исследовательская деятельность в области робототехники должна вестись при соблюдении существующих базовых прав и реализовываться в интересах благополучия и самоопределения личности и общества в целом[4]. Правительством Российской Федерации схожая мысль сформулирована в Концепции регулирования отношений в сфере технологий искусственного интеллекта более определенно: подход к регулированию таких отношений необходимо выстраивать на принципе обеспечения баланса интересов разработчиков, потребителей и иных лиц, а также определения границ их ответственности за возможные негативные последствия использования технологий искусственного интеллекта[5]. Таким образом, во главу угла ставятся не права роботов, а защита физических лиц.

Даже признавая преждевременным положительное решение вопроса о правосубъектности роботов, нужно согласиться с мыслью «о необходимости сработать на опережение, нормативно закрепить обязанность разработчиков и других уполномоченных лиц предпринимать все необходимые меры, обеспечивающие в процессе функционирования искусственного интеллекта интересы человека, и разработать систему норм, обеспечивающих исполнение этой обязанности» (Дурнева, 2019).

Приоритет защиты прав человека даже при регулировании такой специфической сферы, как деятельность искусственного интеллекта, важна в силу еще одного

---

4 European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

5 Распоряжение Правительства Российской Федерации № 2129-р от 19.07.2020. Собрание законодательства Российской Федерации, (2020). 35, ст. 5593.

аспекта. Тот факт, что результаты обработки информации роботом сопоставимы, а зачастую и превосходят аналогичные результаты человека, вовсе не означает, что сущность обработки информации, т. е. мыслительной работы, искусственного интеллекта сопоставима с мыслительной работой человека. А значит, обоснованными являются сомнения в том, что для искусственного интеллекта присуще осознание ценностного измерения права.

Речь идет не о понимании ценности права как одной из аксиом, которую искусственный интеллект может использовать для обработки данных. Речь идет именно об осознании этой ценности, т. е. о субъективном отношении к ней. Проще говоря, нужны ли искусственному интеллекту права? С точки зрения логики развитого гражданина ответ однозначен: любому действующему и осознающему себя субъекту права нужны. Но так ли однозначен этот ответ с точки зрения самого искусственного интеллекта? Иными словами, присваивая роботу права, не навязываем ли мы ему сугубо чуждую категорию, не обладающую для него каким бы то ни было ценностным измерением?

В рамках дискуссии о правосубъектности, правоспособности и деликтоспособности искусственного интеллекта необходимо, по крайней мере, обозначить такой важный аспект, как осознание себя субъектом права. Ведь самоидентификация отнюдь не тождественна предзаписанному и предопределенному алгоритмом ответу «Я субъект права». Такой ответ технически сегодня может озвучить любая умная колонка. Но можем ли мы быть уверенными в том, что для решений искусственного интеллекта имеет хоть какое-нибудь значение то, что скрывается за этими словами?

В перспективе нельзя совершенно исключать возникновения действительной необходимости признания и регулирования прав искусственного интеллекта на созданные им произведения. Однако не менее вероятным даже в перспективе представляется поиск альтернативных вариантов фиксации и защиты устойчивой связи между искусственным интеллектом и результатами его деятельности – ведь право является чрезвычайно значимым, но отнюдь не единственным институтом регулирования отношений. Представляется, что поиск регуляторного института, онтологически релевантного феномену искусственного интеллекта, станет актуальным вопросом в самом ближайшем будущем.

Эти базовые соображения относительно правовой субъектности чрезвычайно важны для точного рассмотрения вопроса об авторских правах искусственного интеллекта на созданные им произведения.

2. Робот как инструмент творчества

Робот пишет музыку. Робот пишет картины. Робот пишет рассказы. Наконец, робот пишет программный код. Зачастую он делает все это не хуже человека. И уж точно делает гораздо быстрее.

Велик соблазн поставить знак равенства между созданием произведений, традиционно относящихся к объектам авторского права, и творчеством. В правовой сфере ставится вопрос о признании за искусственным интеллектом авторских прав и об указании его в качестве правообладателя (Abbott, 2016), ведь творческий вклад в создание произведения традиционно рассматривается в качестве ключевого признака авторства. И по большому счету дискуссия о корректности указания авторства

искусственного интеллекта на произведение, созданное с его участием, продолжается по сей день.

Примечательно в этом контексте известное дело доктора Стивена Тейлера, которое рассматривалось судами в нескольких странах общего права. Он утверждал, что создал машину для изобретений. Эта машина разработала несколько полезных моделей, которые доктор Тейлер решил запатентовать. Причем в качестве патентообладателя он указал себя на том основании, что изобретения были сделаны машиной, которая принадлежала ему.

Патентное ведомство Великобритании отказало ему в регистрации такого права, и этот отказ изобретатель обжаловал в суде. По его словам, действующее законодательство об охране авторского права не содержит положения о том, что права изобретателя должны принадлежать именно человеку. Принадлежность же патентных прав собственнику машины он обосновывал по аналогии с правилом о приращении собственности: «Приплод принадлежит хозяину стада».

Дело «Тейлер против Генерального контролера по патентам, товарным знакам и промышленным образцам» дошло до Апелляционного суда Англии и Уэльса, который 21 сентября 2021 г. вынес вердикт о том, что нормы действующего патентного законодательства не позволяют считать искусственный интеллект автором изобретения[6]. Зато когда Тейлер обратился в австралийский суд с иском к местному патентному ведомству, то судья поддержал его позицию о том, что искусственный интеллект можно и нужно признавать изобретателем[7], а без предоставления правовой охраны изобретениям искусственного интеллекта не будет достигнута сама цель патентного законодательства в виде поощрения технического прогресса.

Этот спор демонстрирует нам то, что теоретический, на первый взгляд, вопрос об авторстве искусственного интеллекта распадается на два прикладных вопроса:

1. Можно ли считать искусственный интеллект автором изобретения, художественного произведения и т. п.?

2. Если искусственный интеллект автором считать нельзя, то подлежит ли такое произведение охране в качестве объекта авторского права?

Для ответа на оба эти вопроса уместно будет в продолжение обзора прецедентов системы общего права вспомнить стародавнее дело «Литографическая компания Берроу-Джайлз против Сарони». Верховный суд Соединенных Штатов Америки 17 марта 1884 г. в решении по этому делу признал авторские права на фотокарточку не за фотоаппаратом и не за его изготовителем, а за фотографом[8].

Мы не можем сегодня достоверно судить о том, казался ли в последней четверти XIX в. фотоаппарат футуристической технологией в той же мере, в какой искусственный интеллект кажется в первой четверти XXI в. Но чрезвычайно актуальным представляется вывод суда о том, что именно фотограф задумал, организовал исполнение и воплотил в жизнь творческий замысел. Пусть и сделал он это при помощи фотоаппарата

---

6 Judgment of the Court of Appeal in England and Wales in Thaler vs Comptroller-General of Patents, Designs and Trademarks [2021] EWCA Civ. 1374. https://clck.ru/36hASY

7 Judgment the Federal Court of Australia in Thaler v. Commissioner of Patents [2021] FCA 879. https://clck.ru/36hAT8

8 Burrow-Giles Lithographic Co. v. Sarony. March 17, 1884. https://clck.ru/36hATk

И в самом деле, фотограф не тождествен художнику – но это не мешает им обоим быть авторами. Композитор может создавать музыку при помощи синтезатора – но именно он является автором этой музыки. Ни у кого не вызывает сомнения то, что в первом случае речь идет лишь о способе нанесения изображения, а во втором лишь о способе звукоизвлечения, а никак не о передаче человеком части своей творческой работы инструменту.

Более того, чем меньше труда автора тратится на подготовку красок и мольберта либо на организацию оркестра духовых инструментов, тем в большей степени сущность этого труда составляет собственно творчество. Идея, творческий замысел, образ – вот то, с чем работает тот автор, труд которого очищен от ремесленной компоненты.

Искусственный интеллект в этом контексте предстает таким же инструментом, как фотоаппарат. Только инструмент этот предоставляет художнику еще большее пространство для творчества. При этом создание произведений искусства с помощью искусственного интеллекта не отменит и не подменит собой ни живописи, ни фотографии – точно так же, как книгопечатание не отменило каллиграфии.

До тех пор, пока не искусственный интеллект, а именно человек задает параметры будущих произведений, «спорно признавать за искусственным интеллектом авторское право. Авторское право может быть за пользователем искусственного интеллекта, т. е. создателем произведения посредством систем искусственного интеллекта. Уравнивать в правах систему искусственного интеллекта и человека неправомерно» (Ивлиев, Егорова, 2022). Параметры, заданные человеком посредством ввода запроса в чат или иным способом взаимодействия с искусственным интеллектом, прямо влияют и на содержание произведения, и на его качество. Рисовать картины с помощью нейросети или писать тексты с помощью чата без первоначального творческого импульса невозможно.

И не требуется правовой фикции для того, чтобы признать: автором работы, созданной с использованием искусственного интеллекта, является человек, творческую идею которого воплощает эта работа.

В этом контексте устаревшими представляются правовые позиции, согласно которым результаты работы искусственного интеллекта вообще не подлежат охране в качестве объектов интеллектуальной собственности на том основании, что они не созданы человеком. Например, в Соединенных Штатах Америки по теологическим и этическим мотивам сама возможность творчества признается лишь за человеком и не может быть признана ни за одним иным субъектом – ни за природой, ни за животным, ни за машиной (Solum, 1992). Картина, созданная нейросетью, в такой парадигме не подлежит правовой охране в той же степени, что и рисунок мороза на стекле, и отпечаток кошачьей лапы на холсте.

Пленум Верховного Суда Российской Федерации в п. 80 Постановления «О применении части четвертой Гражданского кодекса Российской Федерации» руководствуется той же логикой: «Судам при разрешении вопроса об отнесении конкретного результата интеллектуальной деятельности к объектам авторского права следует учитывать, что по смыслу ст. 1228, 1257 и 1259 Гражданского кодекса Российской Федерации (далее – ГК РФ) в их взаимосвязи таковым является только тот результат, который создан творческим трудом. <...> Результаты, созданные с помощью технических средств при отсутствии творческого характера деятельности человека (например, фото- и видеосъемка работающей в автоматическом режиме камерой

видеонаблюдения, применяемой для фиксации административных правонарушений), объектами авторского права не являются»[9].

Но если камера слежения, фиксирующая работу турникета, и в самом деле не порождает объект авторского права за отсутствием творческой идеи, то уже упомянутые выше картины нейросети или тексты чата не создаются без этой самой идеи. А значит, автором такого произведения можно и должно признавать человека, задавшего искусственному интеллекту эту идею. Нельзя согласиться с выводом о том, что «в деятельности искусственного интеллекта по созданию результатов, похожих на объекты авторского права, отсутствует творчество, поэтому созданные им результаты не могут быть квалифицированы в качестве объектов авторского права и не подлежат охране правом интеллектуальной собственности» (Витко, 2019).

«Производные результата использования программ искусственного интеллекта могут быть признаны объектами гражданского права» (Кирсанова, 2022). Отказ от этого принципа сегодня означал бы отказ в правовой защите огромному числу объектов интеллектуальной собственности, что, в свою очередь, означало бы необоснованное ограничение авторских прав тех граждан, которые могут и должны признаваться их авторами.

Разумеется, можно прогнозировать в будущем ситуации, при которых искусственный интеллект по своей инициативе создал произведение, «похожее на объект авторского права»: например, в ходе выполнения алгоритма по созданию проектной документации пришел к выводу о том, что документация будет неполной без пятиминутного фильма о будущем объекте. Но сегодня по самой своей природе произведения, созданные с использованием искусственного интеллекта, не просто похожи на объекты авторского права, а являются таковыми.

Статья 1228 ГК РФ именно творческий труд называет фактором возникновения авторского права, при этом никак не ограничивая правовую охрану результатов такого труда кругом средств его реализации. Более того, ст. 1227 ГК РФ прямо говорит о том, что авторство не зависит от материального носителя произведения.

При этом наличие творческого труда, результатом которого является авторство на некоторый объект интеллектуальной собственности, вовсе не исключает того, что сам этот объект как художественное произведение будет сугубо вторичным по отношению к ранее созданному иному произведению. При этом сам факт вторичности произведения не может и не должен исключать возможности его правовой охраны. Удачный пример: «Если виртуальная копия (движущийся герой на картине) будет являться новым творческим объектом благодаря определенным эффектам, движениям, мимике или другим творческим действиям, ее можно признать новым производным объектом» (Рахматулина, 2019). Этот нюанс важен при определении охраноспособности произведений искусственного интеллекта, ведь почти каждое из них в той или иной степени базируется не только на творческом замысле человека, составившего запрос для искусственного интеллекта, но и на обработке массива ранее созданных произведений.

Каждое из произведений в этом массиве является объектом авторского права, даже если это право не коммерциализировано и произведения находятся в открытом

[9] Постановление Пленума Верховного Суда Российской Федерации № 10 от 23.04.2019. (2019). Бюллетень Верховного Суда Российской Федерации, 7.

доступе без ограничений на воспроизведение. Более того, уже сейчас актуальна ситуация, при которой нейросеть для создания произведения будет обрабатывать в том числе произведения, ранее созданные другими нейросетями. И эта обработка в ряде случаев может означать заимствование, более или менее заметное для человека.

Дабы не порождать споры о проценте и существе заимствований, неизбежные в случае применения традиционных подходов к защите авторских прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта, представляется крайне важным учитывать этот нюанс при характеристике уникальности таких произведений. Эта уникальность, как уже было сказано выше, порождается не обработкой нейросетью чужих произведений, а тем самостоятельным творческим импульсом, который человек как автор произведения задал нейросети для его создания.

Этот импульс сегодня, как правило, формулируется в виде запроса, представляющего собой сочетание ключевых слов. Для создания любого законченного произведения, представляющего самостоятельную ценность, обычно требуется серия запросов. Именно эти запросы в сочетании с результатом их обработки нейросетью и представляют собой ту уникальную комбинацию, которая и должна стать в перспективе объектом интеллектуальной собственности на произведение, созданное с использованием искусственного интеллекта. Таким образом, при идентификации произведения, созданного нейросетью, целесообразным представляется указывать, по крайней мере, следующие данные:

– имя автора;
– название произведения;
– название нейросети;
– последовательность запросов, заданных автором нейросети.

В случае принятия этой конструкции при идентификации произведения, созданного с использованием искусственного интеллекта, мы будем иметь комбинацию вида «Дмитрий Казанцев, картина “Безмятежность”, сгенерирована по запросу “закат солнца ранней осенью в южных предгорьях Альп” нейросетью Кандинский». Подобную комбинацию целесообразно использовать как при указании авторства на такое произведение, так и при регистрации прав на него в патентных учреждениях в том случае, если нормы национального законодательства предусматривают подобную регистрацию на данную категорию произведений – например, если с помощью нейросети была создана программа для ЭВМ.

Стоит вспомнить о том, что еще в 2017 г. А. Гурко были предложены ряд корректировок в гражданское законодательство для фиксации интеллектуальных прав на результаты деятельности искусственного интеллекта. Так, например, ст. 1228 ГК РФ предлагалось дополнить нормами о то, что права на результаты деятельности искусственного интеллекта возникают у собственника программно-аппаратного комплекса, у правообладателя искусственного интеллекта как программы для ЭВМ либо у пользователя этой программы. В отдельной статье предлагалось сгруппировать нормы, согласно которым права на сгенерированные искусственным интеллектом произведения науки, литературы и искусства принадлежат собственнику устройства, использованного для этой цели, а если собственник устройства не является пользователем использованных для таких целей программ для ЭВМ, то права на такие произведения принадлежат именно пользователю искусственного интеллекта (Гурко, 2017).

За прошедшие несколько лет стала очевидна необходимость известного уточнения этих новелл (например, раскрытия понятия «пользователь» применительно к соотношению прав пользователя и правообладателя). Например, сегодня вполне себе обыденной является схема: работодатель дает задание сотруднику – сотрудник формулирует запрос для нейросети – нейросеть создает произведение. Важно однозначно и на законодательном уровне урегулировать вопрос о том, кто в данном случае является правообладателем. Общий тезис о том, что правами на результаты работы искусственного интеллекта обладает его пользователь, в данном случае является упрощением и требует конкретизации. При этом очевидно, что произведение, созданное с участием искусственного интеллекта, и в этом случае должно обладать правовой защитой.

Но актуальной представляется центральная идея о том, что результатам работы искусственного интеллекта – в том числе в виде художественных произведений, изобретений, полезных моделей, программ для ЭВМ и иных объектов авторского права – логично предоставлять правовую охрану как интеллектуальной собственности конкретного физического или юридического лица.

Другое дело, что использование такого инновационного и специфического инструмента, как искусственный интеллект, требует логического и терминологического обособления созданных с его помощью произведений. Удачным представляются, например, термины «цифровое» или «алгоритмическое» (Mazzone & Elgammal, 2019) искусство. В качестве родового определения более или менее повсеместно используется понятие «результаты деятельности искусственного интеллекта».

Важно лишь не смешивать понятия «результаты деятельности искусственного интеллекта» и «произведения искусственного интеллекта»: в первом случае речь идет об использовании искусственного интеллекта в качестве инструмента, что корректно, тогда как во втором случае можно предположить творческую субъектность искусственного интеллекта, что в настоящее время с учетом существующих технологий преждевременно. Международные исследования ставят под вопрос корректность самого именования нейросетей полноценным искусственным интеллектом и признавать за ними возможность полноценного мышления и решения творческих задач (Lee et al., 2021). И в самом деле, при всей обширности возможностей по обработке информации результаты деятельности искусственного интеллекта сводятся, в сущности, не к созданию новых произведений, а к глубокой компиляции ранее созданных произведений.

Говоря об априорной вторичности таких результатов по отношению к ранее созданным произведениям, нельзя обойти вопрос о границах использования этих ранее созданных произведений при работе с результатом деятельности искусственного интеллекта. Разрешение этого вопроса находится за пределами данной статьи, однако его обозначение представляется необходимым. Например, в 2023 г. стали вирусными созданные нейросетью короткие видео, в которых герои культовых произведений художественной литературы передаются в необычной стилистике – от атмосферы традиционных семей Неаполя до атмосферы фильмов Тарковского.

Очевидно, что для потребителя такие произведения представляют интерес не только и не столько в силу заданной нейросети оригинальной идеи необычной комбинации, сколько в силу использования для этой комбинации популярных образов. И в случае коммерциализации подобных результатов деятельности искусственного интеллекта с неизбежностью встанет вопрос о допустимости использования чужих

образов, обладающих признанной коммерческой значимостью, для создания своих произведений, пусть даже с использованием искусственного интеллекта. Представляется, что на сегодня решение этого вопроса, по крайней мере на концептуальном уровне, может базироваться на существующих подходах и нормах защиты интеллектуальной собственности.

3. Робот как субъект творчества

Сегодня правовая субъектность при создании произведений и авторские права даже на произведения, созданные с использованием искусственного интеллекта, являются прерогативами человека. Но, даже постулируя сегодня такой подход как правило, можно ли быть уверенными в том, что для этого правила не появится исключений? Не стоит ограничиваться лишь сегодняшними реалиями и полностью исключать возможность ситуации, в которой фактическим автором изображения, произведения, мелодии или программ для ЭВМ является именно искусственный интеллект.

Технически уже сегодня такую ситуацию можно себе представить по меньшей мере в двух случаях.

Во-первых, тогда, когда формулировка человеком задания для искусственного интеллекта настолько общая, что не позволяет признать наличие творческого замысла («напиши веселую мелодию», «сделай красивый узор в ориентальном стиле»). Очевидно, что подобные идентичные запросы могут быть сгенерированы едва ли не одновременно огромным количеством пользователей, что делает чрезвычайно затруднительным признание авторского приоритета за одним из них.

Во-вторых, уже сегодня несложно представить ситуацию, когда робот создает потенциальный объект, подлежащий правовой защите в качестве объекта интеллектуальной собственности, вообще без прямого указания на то со стороны человека. Например, человек дает задание на написание технической документации (авторство которого при принятии изложенных выше допущений может быть признано за человеком), а искусственный интеллект в качестве дополнения к такой документации пишет скрипт для расчета рисков (и за этой программой для ЭВМ, созданной искусственным интеллектом, едва ли может быть признано авторство человека хотя бы в силу отсутствия какого бы то ни было творческого замысла со стороны последнего).

Далее речь пойдет не вообще о произведениях, созданных с использованием искусственного интеллекта, а именно о тех результатах работы искусственного интеллекта, в создании которых исчезающе мала роль творческого участия человека или такое участие вовсе затруднительно обозначить. Коль скоро результаты интеллектуальной деятельности искусственного интеллекта потенциально могут создаваться без творческого участия человека, то при обсуждении статуса таких специфических произведений перед нами возникают следующие важные вопросы:

1. Кто является автором произведения, созданного искусственным интеллектом без творческого участия человека?

2. Подлежат ли правовой охране такие результаты деятельности искусственного интеллекта?

Самым простым ответом на эти вопросы может показаться признание всех прав на такое произведение за искусственным интеллектом. Однако, возвращаясь к вопросу о правовой субъектности искусственного интеллекта, мы должны помнить, что

такое простое, на первый взгляд, решение «предполагает не только признание того, что нейросеть создала оригинальное произведение, но также и того, что она способна принимать осознанные решения по распоряжению правами на него» (Коданева, 2021).

В этих условиях можно предложить указывать на авторство искусственного интеллекта в названии произведения, но при этом не рассматривать искусственный интеллект в качестве автора и правообладателя произведения в гражданско-правовом смысле этого слова.

При решении вопроса о правовой охране результатов деятельности искусственного интеллекта стоит однозначно уяснить то, что права на произведения не ограничиваются правом указания авторства. Более того, справедливо замечание: «Авторство результата интеллектуальной деятельности может иметь ценность как титул (изобретатель пенициллина, автор книги «Война и мир» и т. д.), однако коммерческий интерес представляют именно исключительные права» (Петраков, Тумаков, 2022).

И в самом деле, помимо права на указание авторства, существуют – имеют в ряде случаев очевидную прикладную и коммерческую ценность – такие права на результаты интеллектуальной деятельности, как «право на неприкосновенность произведения, право на обнародование, право на отзыв, право на неприкосновенность исполнения; и иные права (например, право следования, право доступа, право на вознаграждение за служебный результат интеллектуальной деятельности, право на защиту фонограммы от искажения при ее использовании, право на получение патента и др.)»[10].

И формулировка гражданско-правовых норм, и правовая доктрина, и практика защиты интеллектуальной собственности говорят нам о том, что автором произведения может быть одно лицо, а обладать правами на такое произведение, в том числе исключительными правами, будет другое лицо. Из этого можно сделать вывод о том, что право на указание авторства обособлено от исключительных прав на произведение.

Таким образом, отсутствие у искусственного интеллекта авторских прав на созданное им произведение – или, если угодно, редуцирование таких прав до обязательного указания того факта, что данное произведение является результатом работы искусственного интеллекта, – не должно означать отсутствие правовой защиты у такого произведения. Вопрос лишь в том, кто же будет в данном случае правообладателем.

Самым очевидным вариантом является рассмотрение результатов деятельности искусственного интеллекта в качестве частного случая служебного произведения, разве что вместо работника, которому работодатель дает служебное задание, в данном случае выступает искусственный интеллект (Yanisky-Ravid, 2017). И в самом деле, правовые последствия в обоих случаях будут схожими: правообладателем становится не автор произведения, а субъект, ставший инициатором его создания. Однако подобие в данном случае не означает тождества. Так, искусственный интеллект не находится в трудовых отношениях со своим правообладателем, запрос правообладателя не оформляется по правилам служебного произведения, сам запрос может вообще не содержать ключевых параметров будущего произведения и т. д.

Вопрос об отличиях служебного произведения от запроса для нейросети не может рассматриваться как исключительно юридико-теоретический. Его практическая значимость обуславливается стремительным распространением технологий

[10] Постановление Пленума Верховного Суда Российской Федерации № 10 от 23.04.2019. (2019). Бюллетень Верховного Суда Российской Федерации, 7.

искусственного интеллекта на производствах. Произведения, созданные искусственным интеллектом в рамках коммерческой деятельности юридического лица, едва ли не в первую очередь являются теми объектами интеллектуальной собственности, права на которые обладают коммерческой ценностью.

Все это заставляет не с теоретической, а с практической точки зрения подходить к решению вопроса, что «введение права на результат деятельности искусственного интеллекта может строиться по модели смежного права, однако оно явно теряет свою связь с авторским правом, а потому уместно, на наш взгляд, в данном ключе говорить о праве sui generis на цифровые результаты деятельности искусственного интеллекта» (Харитонова, 2019). И в самом деле, в том случае, когда авторство на результаты деятельности искусственного интеллекта невозможно признать за конкретным лицом или группой лиц, правовая защита таких результатов требует новых правовых инструментов. Эти инструменты могут и должны строиться на существующих конструкциях интеллектуального права, однако они не могут быть сведены ни к одной такой структуре.

В данной парадигме целесообразным представляется согласие с тезисом «о существовании предпосылок для появления в праве интеллектуальной собственности нового правового института – института права на результаты деятельности искусственного интеллекта. Институт является sue generis в рамках права интеллектуальной собственности и не сводится к традиционному авторскому, патентному праву, институту смежных прав и других, хотя в определенной части и основывается на конструкциях таких традиционных институтов» (Аникин, 2022).

Таким образом, в том случае, когда за человеком можно признать авторство на результаты деятельности искусственного интеллекта и, соответственно, сам искусственный интеллект можно признать лишь инструментом реализации творческого замысла человека, тогда правовая защита произведения может строиться на существующих нормах авторского права. Тогда же, когда подобное признание по тем или иным причинам станет затруднительно, в перспективе потенциально потребуется новый правовой институт. Важно не рассматривать два этих подхода в качестве конкурирующих. Ведь лишь на их сочетании и применении каждого из них в релевантной ситуации и должно строиться будущее право на результаты деятельности искусственного интеллекта.

Выводы

При формулировке выводов относительно правового регулирования и правовой защиты результатов деятельности искусственного интеллекта необходимо прежде всего отдавать себе отчет в том, что эта область в известной степени эластична. Результаты, актуальные сегодня, должны в будущем регулярно поверяться достигнутым уровнем технологий.

Однако сегодня при регулировании авторских прав на тексты, изображения, музыкальные и иные произведения, созданные с использованием искусственного интеллекта, рационально исходить прежде всего из преобладания отсутствия у искусственного интеллекта правовой субъектности. Это не означает принципиальной невозможности признания искусственного интеллекта в качестве субъекта права. Это означает лишь то, что сегодня как с точки зрения существующих цифровых технологий, так и с точки зрения правосознания, деликтоспособности и иных правовых институтов по меньшей мере сомнительной представляется возможность реализации роботом своей правовой субъектности.

«Придание роботам (системе искусственного интеллекта) статуса субъекта права не повлечет за собой в обозримом будущем каких-то явных негативных последствий. В то же время не видны и преимущества такого решения по сравнению с рассмотрением роботов (систем искусственного интеллекта) в качестве квазисубъектов права. Исходя из философского принципа Оккама не умножать сущности без крайней на то необходимости, мы полагаем, что введение в правовую сферу такого принципиально нового субъекта права, как робот (система искусственного интеллекта), является преждевременным (хотя не исключено, что такая необходимость появится)» (Чаннов, 2022).

Выполнение роботом интеллектуальных и творческих задач на уровне, сопоставимом, а иногда и превосходящем уровень человека, нельзя рассматривать в качестве основания для признания искусственного интеллекта идентичным человеку как с точки зрения права в целом, так и с точки зрения авторских прав в частности. «Безусловно, разрыв между искусственным интеллектом и человеком сокращается. Тем не менее, по-видимому, в ближайшее время он не будет полностью преодолен, поскольку именно человек настраивает модель, подбирает обучающие примеры и использует цифровые технологии для творчества. Идея о том, что машины могут быть художниками или могут даже заменить художников, как они уже заменили некоторые профессии, выглядит пока слишком смелой»[11]. При этом сфера творчества в силу самой свой специфики диктует нам осторожность в вопросе о перенесении на искусственный интеллект антропоморфных черт, в том числе присвоении ему категории творчества.

«Наделение искусственного интеллекта субъектом права помогло бы справиться с проблемой авторства. Однако этот подход кажется непригодным для решения других важных проблем, таких как ответственность. Полагаем, что с точки зрения положений института авторского права ничего не будет достигнуто, поскольку все создает человек своим творчеством, оригинальностью и новыми идеями. Этого можно достичь даже сейчас, переосмыслив доктринальные аспекты, формирующие авторское право, такие как оригинальность и творчество, и определив «решающего» человека, стоящего за произведениями искусства, созданными с помощью искусственного интеллекта» (Сушкова, 2022). Именно творческий замысел человека, а вовсе не инструмент реализации такого замысла должен выступать критерием авторства.

На сегодня, исходя из этих посылок, основные выводы относительно интеллектуальных прав на результаты работы искусственного интеллекта можно сформулировать в виде нескольких базовых тезисов.

Во-первых, представляется преждевременным наделение искусственного интеллекта правовой субъектностью – в том числе в силу очевидных проблем как с осознанием и реализацией своей правоспособности, так и с практической реализацией деликтоспособности.

Во-вторых, практика использования искусственного интеллекта для создания текстов, музыкальных произведений, изображений, программ и прочих объектов авторского права сегодня в большинстве случаев позволяет определить того человека или группу лиц, чей творческий замысел реализуется искусственным интеллектом. В этих условиях признание искусственного интеллекта автором произведения представляется необоснованным.

---

[11] Суетин, Н. (2020, 8 июня). Искусственный интеллект в современном искусстве. Инновационный центр Сколково. https://clck.ru/Ntrio

В-третьих, из отказа в признании искусственного интеллекта автором произведения не должен следовать отказ в правовой защите такого произведения. По общему правилу автором и правообладателем должен признаваться тот человек, творческий замысел которого реализуется с использованием искусственного интеллекта. В этом смысле использование искусственного интеллекта для творчества по сути мало чем отличается от использования для тех же целей иных технических средств – таких, как фотоаппарат, синтезатор и т. п.

В-четвертых, отсутствие онтологической разницы между искусственным интеллектом и тем же фотоаппаратом в контексте творчества не означает отсутствия фактической разницы. В связи с этим актуально использование специальных понятий для результатов творчества, в котором был задействован искусственный интеллект. Это может быть общее понятие «результаты деятельности искусственного интеллекта» или более частные определения, например, «цифровое искусство».

В-пятых, в том случае, когда при создании произведения силами искусственного интеллекта невозможно выделить творческий замысел человека и фактическим автором произведения является искусственный интеллект, это заслуживает специального обозначения в качестве произведения искусственного интеллекта. Такое обозначение заменяет указание авторства в гражданско-правовом смысле этого слова, и такие произведения подлежат правовой охране по специальным правилам. Эти правила, в частности, предусматривают отсутствие указания имени автора и правовую защиту произведения в качестве интеллектуальной собственности владельца искусственного интеллекта. Механизм правовой защиты результатов работы искусственного интеллекта в этом случае может быть подобным служебному произведению, но не тождественным ему.

Наконец, важно учитывать принципы и основы технологии обработки информации искусственным интеллектом – в частности, то, что в сформированных им произведениях неизбежны повторы элементов уже существующих произведений, в том числе созданных искусственным интеллектом. В сочетании с постулированием авторства человека, задавшего искусственному интеллекту ключевые слова для создания произведения, представляется необходимым учет в правовой действительности специфики объекта авторского права, созданного с использованием искусственного интеллекта, а именно: объектом правовой охраны выступает сочетание самого произведения (текста, мелодии, изображения и т. д.), сгенерированного искусственным интеллектом, и тех ключевых слов, которые были заданы автором произведения для такой генерации. Объектом защиты авторского права в данном случае будет выступать уникальное сочетание имени автора, последовательности его запросов искусственного интеллекта и самого произведения, сформированного искусственным интеллектом в результате обработки последовательности этих запросов.

Сочетание этих подходов поможет не только выработать адекватное регулирование результатов работы искусственного интеллекта, но и сделать такие результаты полноценным элементом правового поля и в этом смысле полноценной интеллектуальной собственностью. А коль скоро правовая защита является важным фактором интереса и приложения инвестиций, что наглядно демонстрирует, например, патентное право, стоит надеяться на то, что продуманное правовое регулирование интеллектуальных прав на произведения, созданные с участием искусственного интеллекта, послужит импульсом к прогрессу в этой сфере.

Список литературы

Аникин, А. С. (2022). К вопросу об охраноспособности результатов деятельности искусственного интеллекта как объекта интеллектуальной собственности. *Цивилист*, *2*(38), 25–31. https://www.elibrary.ru/kuiptf

Витко, В. (2019). Анализ научных представлений об авторе и правах на результаты деятельности искусственного интеллекта. *Интеллектуальная собственность*. *Авторское право и смежные права*, *3*, 5–22. https://www.elibrary.ru/jsfbce

Гурко, А. (2017). Искусственный интеллект и авторское право: взгляд в будущее. *Интеллектуальная собственность*. *Авторское право и смежные права*, *12*, 7–18. https://www.elibrary.ru/zukikl

Дурнева, П. Н. (2019). Искусственный интеллект: анализ с точки зрения классической теории правосубъектности. *Гражданское право*, *5*. https://doi.org/10.18572/2070-2140-2019-5-30-33

Ивлиев, Г. П., Егорова, М. А. (2022). Юридическая проблематика правового статуса искусственного интеллекта и продуктов, созданных системами искусственного интеллекта. *Журнал российского права*, *6*, 32–46. https://doi.org/10.12737/jrl.2022.060

Кирсанова, Е. Е. (2022). *Правовое регулирование оборота прав на результаты интеллектуальной деятельности в цифровой экономике*. Москва: Юстицинформ. https://www.elibrary.ru/rfcgjq

Коданева, С. И. (2021). Трансформация авторского права под влиянием развития цифровых технологий. *Право и цифровая экономика*, *4*(14). https://doi.org/10.17803/2618-8198.2021.14.4.031-038

Петраков, Н. А., Тумаков, А. В. (2022). Проблемы правовой охраны объектов, созданных с использованием технологий искусственного интеллекта. *Цивилист*, *4*(40), 16–18. https://www.elibrary.ru/wtcbcj

Рахматулина, Р. Ш. (2019). Цифровая форма объектов авторского права. *Право и цифровая экономика*, *1*. https://doi.org/10.17803/2618-8198.2019.03.1.035-038

Сушкова, О. В. (2022). Правовые средства оборота объектов, созданных с использованием технологий искусственного интеллекта. *Гражданское право*, *2*. https://doi.org/10.18572/2070-2140-2022-2-12-15

Харитонова, Ю. С. (2019). Правовой режим результатов деятельности искусственного интеллекта. В кн. Е. Б. Лаутс (отв. ред.), *Современные информационные технологии и право*, 68–83. Москва: Статут.

Чаннов, С. Е. (2022). Робот (система искусственного интеллекта) как субъект (квазисубъект) права. *Актуальные проблемы российского права*, *12*. https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Abbott, R. (2016). I Think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, *57*. https://doi.org/10.2139/ssrn.2727884

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Calo, R., Chizeck, H. J., Joh, E., & Hannaford, B. (2018). Panel 2: Accountability for the Actions of Robots. *Seattle University Law Review*, *41*, 1101. https://clck.ru/36pgAM

Cofone, I. (2018). Servers and Waiters: What Matters in the Law of AI. *Stanford Technology Law Review*, *21*, 167. https://doi.org/10.31228/osf.io/2nstf

Colonna, K. (2012). Autonomous Cars and Tort Liability. *Case Western Reserve Journal of Law, Technology & the Internet*, *4*(4). https://doi.org/10.2139/ssrn.2325879

Duffy, S. H., & Hopkins, J. P. (2017). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*(3), 453–480. https://clck.ru/36pgCG

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property.* Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Mazzone, M., & Elgammal, A. (2019). Art, Creativity, and the Potential of Artificial Intelligence. *Arts*, *8*(1). https://doi.org/10.3390/arts8010026

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287. http://scholarship.law.unc.edu/nclr/vol70/iss4/4

Yanisky-Ravid, Sh. (2017). Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – the HumanLike Authors Are Already Here – a New Model. *Michigan State Law Review*, 4. https://doi.org/10.2139/ssrn.2957722

Сведения об авторе

Казанцев Дмитрий Александрович – кандидат юридических наук, руководитель Департамента нормативно-правового регулирования оператора электронной торговой площадки B2B-Center (АО «Центр развития экономики»)
Адрес: 107113, Российская Федерация, г. Москва, 3-я Рыбинская улица, 18/22
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

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: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 15 мая 2023 г.
Дата одобрения после рецензирования – 15 июля 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.39

Copyrights to the Results of Artificial Intelligence Activity and Means of Their Protection

Dmitriy A. Kazantsev

B2B-Center
Moscow, Russian Federation

Keywords

artificial intelligence,
creativity,
delictual dispositive capacity,
digital technologies,
intellectual property,
law,
legal capacity,
legal personality,
neuron network,
robot

Abstract

Objective: to substantiate the mechanisms of legal protection of intellectual property objects created with the use of artificial intelligence.

Methods: the use of artificial intelligence to create works that are traditionally considered copyright objects was investigated with a set of general scientific and theoretical-legal methods of scientific cognition, including comparison, analogy and synthesis. In addition, the practice of using artificial intelligence, including neural networks, to create such works was considered in several aspects on the basis of retrospective and multifactor analysis.

Results: the paper summarizes the current practice of using artificial intelligence to create works that traditionally belong to intellectual property objects (texts, images, music, software), taking into account the formulated scientific and legal positions. Several qualitatively different variants of the use of artificial intelligence were identified. For each of these variants the mechanism of legal protection was proposed and the areas of their effective application were indicated. Proposals were made to regulate the legal protection of the results of artificial intelligence activity; this was made not in the paradigm of competing doctrines, but by combining several tools, each of them to be applied in a relevant situation.

Scientific novelty: the paper presents ontological differentiation of the results of artificial intelligence activity and the corresponding mechanisms of their legal protection. The author propose to consider the results of activity created by artificial intelligence not as a single object of legal regulation, but as a set of externally similar, but ontologically different objects, each requiring a separate approach to legal protection.

Practical significance: the ontological differentiation of the results of artificial intelligence activity and their corresponding legal protection mechanisms proposed in this paper is relevant both as a basis for further research and as proposals to supplement civil legislation.

For citation

Kazantsev, D. A. (2023). Copyrights to the results of artificial intelligence activity and means of their protection. *Journal of Digital Technologies and Law, 1*(4), 909–931. https://doi.org/10.21202/jdtl.2023.39

References

Abbott, R. (2016). I Think, Therefore I Invent: Creative Computers and the Future of Patent Law. *Boston College Law Review*, *57*. https://doi.org/10.2139/ssrn.2727884

Anikin, A. S. (2022). On the protectability of the results of artificial intelligence activity as an object of intellectual property. *Civilist*, *2*, 25–31. (In Russ.).

Bertolini, A. (2013). Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules. *Law, Innovation and Technology*, *5*(2), 214–247. https://doi.org/10.5235/17579961.5.2.214

Calo, R., Chizeck, H. J., Joh, E., & Hannaford, B. (2018). Panel 2: Accountability for the Actions of Robots. *Seattle University Law Review*, *41*, 1101. https://digitalcommons.law.uw.edu/faculty-articles/493

Cofone, I. (2018). Servers and Waiters: What Matters in the Law of AI. *Stanford Technology Law Review*, *21*, 167. https://doi.org/10.31228/osf.io/2nstf

Channov, S. E. (2022). Robot (Artificial Intelligence System) as a Subject (Quasi-Subject) of Law. *Actual Problems of Russian Law*, *12*. (In Russ.). https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Colonna, K. (2012). Autonomous Cars and Tort Liability. *Case Western Reserve Journal of Law, Technology & the Internet*, *4*(4). https://doi.org/10.2139/ssrn.2325879

Duffy, S. H., & Hopkins, J. P. (2017). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*(3), 453–480. https://scholar.smu.edu/scitech/vol16/iss3/4

Durneva, P. N. (2019). Artificial Intelligence: An Analysis from the Standpoint of the Classical Legal Capacity Theory. *Civil law*, *5*. (In Russ.). https://doi.org/10.18572/2070-2140-2019-5-30-33

Greenstein, S. (2022). Preserving the rule of law in the era of artificial intelligence (AI). *Artificial Intelligence and Law*, *30*, 291–323. https://doi.org/10.1007/s10506-021-09294-4

Gurko, A. (2017). Artificial intelligence and copyright law: a glance into the future. *Intellectual Property*, *12*.

Ivliev, G. P., & Egorova, M. A. (2022). Legal Issues of the Legal Status of Artificial Intelligence and Products Created by Artificial Intelligence Systems. *Journal of Russian Law*, *6*, 32–46. (In Russ.). https://doi.org/10.12737/jrl.2022.060

Kharitonova, Yu. S. (2019). legal regime of the results of artificial intelligence functioning. In E. B. Lauts (Ed.), *Modern information technologies and law* (pp. 68–82). Moscow: Statut. (In Russ.).

Kirsanova, E. E. (2022). *Legal regulation of the turnover of right to the results of intellectual activity in digital economy*. Moscow: Yustitsinform.

Kodaneva, S. I. (2021). Transformation of copyright under the development of digital technologies. *Law and Digital Economy*, *4*(14). https://doi.org/10.17803/2618-8198.2021.14.4.031-038

Lee, J-.A., Hilty, R., & Liu, K-.C. (Eds.). (2021). *Artificial intelligence and intellectual property.* Oxford University Press. https://doi.org/10.1093/oso/9780198870944.001.0001

Mazzone, M., & Elgammal, A. (2019). Art, Creativity, and the Potential of Artificial Intelligence. *Arts*, *8*(1). https://doi.org/10.3390/arts8010026

Petrakov, N. A., & Tumakov, A. V. (2022). The problems of legal protection of objects created with the use of artificial intelligence technologies. *Civilist*, *4*. (In Russ.).

Rakhmatulina, R. Sh. (2019). Electronic Form of copyright Items. *Law and Digital Economy*, *1*. (In Russ.). https://doi.org/10.17803/2618-8198.2019.03.1.035-038

Solaiman, S. M. (2017). Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy. *Artificial Intelligence and Law*, *25*. https://doi.org/10.1007/s10506-016-9192-3

Solum, L. B. (1992). Legal Personhood for Artificial Intelligences. *North Carolina Law Review*, *70*(4), 1231–1287. http://scholarship.law.unc.edu/nclr/vol70/iss4/4

Sushkova, O. V. (2022). Legal Means of Circulation of Objects Created with the Use of Artificial Intelligence Technologies. *Civil Law*, *2*. (In Russ.). https://doi.org/10.18572/2070-2140-2022-2-12-15

Vitko, V. (2019). Analysis of scientific views of authorship and right for results of ai activity (continued). *Intellectual Property*, *3*, 5–22. (In Russ.).

Yanisky-Ravid, Sh. (2017). Generating Rembrandt: Artificial Intelligence, Copyright, and Accountability in the 3A Era – the HumanLike Authors Are Already Here – a New Model. *Michigan State Law Review*, *4*. https://doi.org/10.2139/ssrn.2957722

Author information

Dmitriy A. Kazantsev – Cand. Sci. (Law), Head of the Department of normative-legal regulation of the B2B-Center electronic trading platform operator
Address: 18/22 3rd Rybiskaya Str., 107113 Moscow, Russian Federation
E-mail: info@dkazantsev.ru
ORCID ID: https://orcid.org/0000-0003-2182-5776
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=1149755

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 15, 2023
Date of approval – July 15, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:364.25:504.75:004.8
EDN: https://elibrary.ru/ffvrya
DOI: https://doi.org/10.21202/jdtl.2023.40

Воздействие искусственного интеллекта на окружающую среду: скрытые экологические издержки и этико-правовые вопросы

Алеся Жук

Университет Помпеу Фабра
г. Барселона, Испания

Ключевые слова

алгоритмическая предвзятость,
искусственный интеллект,
потребление энергии,
право,
природные экосистемы,
устойчивое развитие,
центр обработки данных,
цифровые технологии,
экологические издержки,
электронные отходы

Аннотация

Цель: выявление скрытых экологических издержек, связанных с разработкой, внедрением и развитием технологий искусственного интеллекта, с целью его устойчивой и гармоничной интеграции с различными секторами экономики путем определения оптимальных нравственно-этических и политико-правовых стратегий.

Методы: в основе проведенного исследования лежит экологический подход к разработке и внедрению искусственного интеллекта, междисциплинарный и политико-правовой анализ экологических проблем и рисков алгоритмической предвзятости, ошибок в алгоритмах искусственного интеллекта и процессах принятия решений, которые могут усугубить экологическое неравенство и несправедливость в отношении к окружающей среде. Кроме того, подвержены анализу вызванные развитием технологий искусственного интеллекта последствия разрушений природных экосистем, обусловленные энергоемким характером связанных с ним вычислений, растущим влиянием центров обработки данных на потребление энергии и проблем с их охлаждением, образование электронных отходов из-за быстрого совершенствования оборудования и др.

Результаты: проведенный анализ показывает разнообразие экологических, этических и политико-правовых проблем, связанных с обучением, использованием и развитием искусственного интеллекта, потребляющего значительное количество энергии (в основном из невозобновляемых источников), что приводит к увеличению выбросов углерода и создает препятствия для дальнейшего устойчивого экологического развития. Неправильная утилизация оборудования искусственного интеллекта усугубляет проблему электронных отходов, загрязнения планеты, еще больше нанося ущерб окружающей среде. Ошибки в алгоритмах искусственного интеллекта и процессах

принятия решений ведут к несправедливости в отношении окружающей среды и экологическому неравенству. Технологии искусственного интеллекта могут нарушать природные экосистемы, ставя под угрозу среду обитания диких животных и модели миграции.

Научная новизна: исследование экологических последствий использования и дальнейшего развития искусственного интеллекта, вызванных в связи с этим экологических нарушений и издержек устойчивого развития позволяет определить научный поиск оптимальных стратегий минимизации вреда окружающей среде, в котором правоведам и юристам предстоит установить этико-правовые и политико-правовые решения на национальном и наднациональном уровнях.

Практическая значимость: понимание экологического воздействия искусственного интеллекта имеет решающее значение для политиков, юристов, исследователей, отраслевых специалистов при разработке стратегий минимизации вреда окружающей среде. Полученные данные подчеркивают важность реализации энергоэффективных алгоритмов, перехода на возобновляемые источники энергии, внедрения ответственной практики обращения с электронными отходами, обеспечения справедливости при принятии решений искусственным интеллектом и учета этических соображений и правил его внедрения.

Для цитирования

Жук, А. (2023). Воздействие искусственного интеллекта на окружающую среду: скрытые экологические издержки и этико-правовые вопросы. *Journal of Digital Technologies and Law*, *1*(4), 932–954. https://doi.org/10.21202/jdtl.2023.40

Содержание

Введение

Искусственный интеллект (далее – ИИ) представляет собой мощный фактор преобразований в различных сферах жизни людей – от здравоохранения до транспорта, от сферы обслуживания до финансовых систем. Благодаря своей способности обрабатывать огромные объемы данных и учиться на основе выявленных закономерностей ИИ открыл новые возможности для инноваций и повышения эффективности. Однако пока человечество восхищается новыми достижениями, необходимо выявить и изучить скрытые экологические издержки, связанные с происходящей технологической революцией.

По мере роста спроса на приложения ИИ увеличивается и потребление энергии, необходимой для питания вычислительной инфраструктуры. По данным исследования Strubell et al. (2019), обучение одной современной модели искусственного интеллекта может привести к выбросу такого количества углекислого газа, которое соответствует выхлопу пяти автомобилей за весь срок службы. Значительный вклад в это энергопотребление вносят центры обработки данных, которые обеспечивают размещение и функционирование ИИ; зачастую они используют невозобновляемые источники энергии. Экспоненциальный рост технологий искусственного интеллекта вызывает тревогу относительно их долгосрочного воздействия на окружающую среду, поскольку экологические издержки, связанные с революцией ИИ, остаются практически неизученными и неучтенными.

Кроме того, быстрое развитие устройств с технологиями искусственного интеллекта приводит к сокращению их жизненного цикла, что влечет за собой резкое увеличение количества электронных отходов. Согласно отчету Global E-waste Monitor 2020, объем электронных отходов достиг рекордных 53,6 млн тонн, при этом только 17,4 % из них официально собираются и перерабатываются[1]. Неправильное обращение с устаревшими аппаратными компонентами ИИ создает значительные экологические риски, способствуя загрязнению окружающей среды и истощению ресурсов.

Технологии искусственного интеллекта обладают огромным потенциалом для экологического мониторинга и природоохранных мероприятий, однако в то же время применение этих технологий может разрушать природные экосистемы. Например, беспилотные летательные аппараты для экологического мониторинга и автономные транспортные средства, используемые для разведки ресурсов, могут нарушить среду обитания диких животных, их миграционные процессы и усугубить дисбаланс экосистем. Непредвиденные последствия воздействия ИИ на биоразнообразие и экосистемы требуют тщательного рассмотрения для обеспечения ответственного и устойчивого применения этих технологий.

В свете этих опасений необходимо более глубоко изучить экологическое влияние технологий искусственного интеллекта и найти стратегии для смягчения их негативного воздействия на окружающую среду. В данной статье рассматриваются различные аспекты экологических издержек, связанных с ИИ, подчеркивается необходимость использования энергоэффективных алгоритмов, ответственной практики утилизации электронных отходов, устойчивой инфраструктуры центров обработки

[1] Forti, V., Baldé, C. P., Kuehr, R., & Bel, G. (2020). The global E-waste monitor 2020. United Nations University (UNU), International Telecommunication Union (ITU) & International Solid Waste Association (ISWA), Bonn/Geneva/Rotterdam, 120.

данных, а также затрагиваются этические аспекты принятия решений в области ИИ. Проливая свет на эти вопросы, статья призвана стимулировать дискуссии и меры, способствующие более экологичному подходу к разработке и внедрению ИИ.

1. Потребление энергии

По мере того как человечество продолжает осваивать возможности искусственного интеллекта, возникает необходимость признать и решить проблему значительного энергопотребления, сопровождающего эту технологическую революцию. В данном разделе рассматривается энергоемкость вычислений ИИ, значительные энергетические потребности центров обработки данных, а также их зависимость от невозобновляемых источников энергии. Проливая свет на скрытые экологические издержки технологической революции в области ИИ, мы сможем глубже понять последствия для окружающей среды, связанные с заметным влиянием ИИ на различные сферы человеческой жизни.

Вычисления в области ИИ известны своими значительными энергозатратами, связанными с обработкой огромных объемов данных и выполнением сложных алгоритмов. В частности, обучение современных моделей ИИ требует большого количества энергии. Так, крупномасштабные модели потребляют до сотен мегаватт-часов, что эквивалентно энергии, необходимой для питания тысяч домохозяйств в течение нескольких месяцев (Strubell et al., 2019). Вычислительные мощности и итерационные процессы, связанные с обучением моделей ИИ, обусловливают их высокое энергопотребление. Эти потребности возникают из-за необходимости обработки больших массивов данных, выполнения сложных матричных операций и оптимизации параметров модели в ходе многочисленных итераций. Понимание энергетического следа вычислений ИИ необходимо для осознания воздействия на окружающую среду, связанного с их широким распространением.

Центры обработки данных (далее – ЦОД) играют важную роль в работе систем искусственного интеллекта, обеспечивая размещение и функционирование вычислительной инфраструктуры. Однако они вносят существенный вклад в общее энергопотребление ИИ. Эти объекты требуют значительного количества электроэнергии для питания серверов, систем охлаждения и сетевого оборудования. Высокопроизводительные вычислительные возможности приводят к повышению энергопотребления таких центров. В работе Hanus et al. (2023) подчеркиваются энергоемкий характер центров обработки данных и проблемы, с которыми они сталкиваются при достижении энергоэффективности. Развитие технологий искусственного интеллекта привело к увеличению числа и масштабов центров обработки данных, что усиливает их воздействие на окружающую среду. Неэффективное использование вычислительных ресурсов и систем охлаждения в ЦОД еще больше увеличивает их энергопотребление и усугубляет негативное воздействие на окружающую среду.

Актуальной проблемой энергопотребления ИИ является зависимость от невозобновляемых источников энергии. Основными источниками электроэнергии для вычислений ИИ являются традиционные электросети, часто работающие на ископаемом топливе. Такая зависимость от невозобновляемых источников энергии увеличивает выбросы парниковых газов и усугубляет экологические проблемы. В работе Şerban et al. (2020) подчеркивается важность перехода на возобновляемые источники энергии для создания устойчивой инфраструктуры ИИ. Использование возобновляемых источников энергии, таких как солнечная или ветровая

энергия, в центрах обработки данных позволяет снизить «углеродный след» систем ИИ и уменьшить их воздействие на окружающую среду. Внедрение технологий возобновляемой энергетики не только сокращает выбросы парниковых газов, но и способствует созданию более устойчивой энергетической инфраструктуры, способной поддерживать растущие потребности в вычислениях с использованием искусственного интеллекта.

1.1. Энергозатратный характер вычислений с помощью искусственного интеллекта

Энергоемкость вычислений в области ИИ вызывает все большую озабоченность в связи со значительными потребностями в энергии, связанными с обучением и запуском сложных моделей искусственного интеллекта (Henderson et al., 2018). По мере развития и усложнения приложений ИИ резко возрастает потребность в вычислительных мощностях, что приводит к увеличению энергопотребления.

Одним из основных факторов, влияющих на энергопотребление вычислений, является этап обучения ИИ. В случае модели глубокого обучения нейронные сети получают огромный объем информации, а затем настраивают свои внутренние параметры с помощью итерационных процессов для оптимизации производительности. Этот процесс обучения часто требует многократных итераций на больших массивах данных с использованием мощной аппаратной инфраструктуры, такой как графические процессоры (GPU) или специализированные тензорные процессоры (TPU) (Strubell et al., 2019).

Эти аппаратные компоненты являются весьма энергоемкими и потребляют значительное количество электроэнергии для выполнения сложных вычислений, необходимых для обучения моделей ИИ. Потребление энергии в процессе обучения может составлять от нескольких сотен до нескольких тысяч киловатт-часов (кВт·ч) в зависимости от размера и сложности модели, объема данных и используемой аппаратной инфраструктуры (Schwartz et al., 2020).

К примеру, в исследовании Schwartz et al. (2020) было показано, что обучение одной современной языковой модели может привести к выбросу такого же количества углекислого газа, как за весь срок службы пяти автомобилей. Это говорит о значительном воздействии на окружающую среду, связанном с энергопотреблением вычислений ИИ.

Помимо этапа обучения, энергопотребления требуют также этапы внедрения и использования моделей ИИ. После обучения модели ее необходимо запустить на различных устройствах или облачных серверах для выполнения конкретных задач в режиме реального времени. Этот этап также требует вычислительных ресурсов, хотя, как правило, менее масштабных по сравнению с обучением. Однако при масштабном использовании моделей ИИ суммарное энергопотребление все равно может быть значительным (Strubell et al., 2019).

Энергоемкость вычислений ИИ вызывает тревогу по поводу воздействия технологий искусственного интеллекта на окружающую среду и их устойчивости. По мере дальнейшего распространения приложений ИИ в различных отраслях промышленности спрос на вычислительные ресурсы будет только расти, что приведет к еще большему увеличению энергопотребления. В связи с этим становятся крайне важными поиск энергоэффективных вычислительных архитектур, разработка алгоритмов,

минимизирующих вычислительные потребности, и использование возобновляемых источников энергии для питания инфраструктуры ИИ (Ding et al., 2021).

В настоящее время предпринимаются усилия для решения этих проблем. Исследователи и эксперты в области промышленности активно работают над созданием более энергоэффективных алгоритмов и аппаратных архитектур, исследуя такие методы, как сжатие моделей, квантование и распределенное обучение. Эти подходы направлены на снижение вычислительных требований моделей ИИ без существенного уменьшения производительности (Ding et al., 2021). Кроме того, все большее внимание уделяется оптимизации функционирования центров обработки данных и использованию возобновляемых источников энергии для питания инфраструктуры ИИ, что позволит сократить углеродный след, связанный с вычислениями ИИ (Strubell et al., 2019).

1.2. Центры обработки данных: энергозатратность инфраструктуры искусственного интеллекта

Центры обработки данных играют важнейшую роль в поддержании инфраструктуры ИИ, являясь основой для хранения и обработки огромных объемов данных. Однако эти центры потребляют очень много энергии, что вызывает озабоченность по поводу их воздействия на окружающую среду (Dhar, 2020).

В центрах обработки данных размещаются серверы, сетевое оборудование и системы хранения данных, необходимые для выполнения вычислительных задач, стоящих перед ИИ. Эти объекты работают круглосуточно, потребляя огромное количество электроэнергии для питания и охлаждения оборудования, а также для обеспечения систем бесперебойного питания для резервного копирования (Shah et al., 2010).

Энергопотребление центров обработки данных зависит от различных факторов, включая количество и эффективность серверов, систем охлаждения и общее устройство инфраструктуры. Серверы и охлаждающее оборудование потребляют значительную часть энергии, причем только на охлаждение приходится до 40 % общего энергопотребления (Masanet et al., 2020). По оценкам исследователей, в 2020 г. центры обработки данных во всем мире потребили от 196 до 400 тераватт-часов (ТВт·ч), что составило около 1 % мирового потребления электроэнергии[2]. Энергоэффективность центров обработки данных стала одним из основных направлений снижения их воздействия на окружающую среду. Ведутся работы по повышению эффективности серверов, оптимизации систем охлаждения и проектированию центров обработки данных с учетом принципов энергосбережения. При этом используются такие технологии, как виртуализация серверов, передовые технологии охлаждения, внедряются новые стратегии управления питанием (Shah et al., 2010).

Кроме того, растет интерес к использованию возобновляемых источников энергии для питания центров обработки данных. Многие компании инвестируют в подобные проекты и приобретают сертификаты возобновляемых источников энергии (renewable energy certificates, REC) для компенсации потребления электроэнергии (Dhar, 2020). Так, в 2017 г. компания Google объявила, что закупленные ею

[2] Garcia, C. (2022). The Real Amount of Energy A Data Center Uses. https://clck.ru/36kxEN

сертификаты возобновляемых источников энергии компенсировали 100 % потребления электроэнергии в центрах обработки данных и офисах компании по всему миру[3].

Для решения энергетических проблем, возникающих в центрах обработки данных, создаются отраслевые коллаборации, нормативные акты и исследовательские проекты. Эти усилия направлены на разработку стандартов, продвижение лучших практик и стимулирование внедрения энергоэффективных технологий в работу центров обработки данных (Shah et al., 2010). Так, в Великобритании над повышением энергоэффективности и обеспечением устойчивого развития индустрии ЦОД активно работает организация Data Centre Alliance[4].

1.3. Невозобновляемые источники энергии и углеродные выбросы

Зависимость инфраструктуры ИИ от невозобновляемых источников энергии существенно влияет на выбросы углерода и на окружающую среду в целом. Производство электроэнергии из ископаемых видов топлива, таких как уголь и природный газ, приводит к выбросам парниковых газов и усугубляет климатические изменения (Ram et al., 2018). По оценкам, выбросы углекислого газа только от центров обработки данных сравнимы с выбросами авиационной промышленности[5].

Центры обработки данных, в которых размещается вычислительная инфраструктура для ИИ, – это чрезвычайно энергоемкие объекты. Они требуют значительного количества электроэнергии для питания серверов, систем охлаждения и другой вспомогательной инфраструктуры. Во многих регионах электроэнергия, используемая для питания центров обработки данных, поступает преимущественно из невозобновляемых источников. Например, в Великобритании значительная часть электроэнергии по-прежнему вырабатывается на ископаемом топливе[6].

Выбросы углерода, связанные с невозобновляемыми источниками энергии, напрямую влияют на «углеродный след» систем ИИ. В исследовании Rolnick et al. (2022) было подсчитано, что обучение большой модели ИИ может привести к выбросу такого же объема углерода, как и у среднего американского автомобиля за весь срок службы.

Для решения этих проблем специалисты по искусственному интеллекту все чаще рассматривают идею перехода на возобновляемые источники энергии и сокращения выбросов углекислого газа. Ряд крупных технологических компаний, в том числе Microsoft и Amazon, взяли на себя обязательства по достижению углеродной нейтральности и использованию возобновляемых источников энергии для своих центров обработки данных[7].

Правительства и организации также предпринимают шаги, способствующие внедрению возобновляемых источников энергии в секторе ИИ. Так, например,

---

3 Google. (2021). Google reaches 100% renewable energy goal. https://clck.ru/36kxG4

4 Data Centre Alliance. (n.d.). About the DCA. https://clck.ru/36kxHA

5 Lim, S. (2022, July 14). Media industry's pollution equivalent to aviation, study finds. Campaign. https://clck.ru/36kxHu

6 Department for Business, Energy & Industrial Strategy. (2020). BEIS Electricity Generation Costs. https://clck.ru/36kxKS

7 Microsoft. (2022). Microsoft announces plan to be carbon negative by 2030. https://clck.ru/36kxLJ ; См. также Amazon. (n.d.). Amazon and Global Optimism announce The Climate Pledge. https://clck.ru/36kxMP

Европейский союз поставил задачу по увеличению доли возобновляемых источников энергии и сокращению выбросов парниковых газов в странах-членах[8].

Кроме того, усилия исследователей направлены на разработку энергоэффективных алгоритмов и аппаратных средств для минимизации энергопотребления и выбросов углекислого газа при вычислениях ИИ. С целью оптимизации энергоэффективности систем ИИ изучаются такие методы, как сжатие модели, квантование и специализированные аппаратные архитектуры (Strubell et al., 2019).

1.4. Необходимость разработки энергоэффективных алгоритмов и устройств с технологией искусственного интеллекта

Поскольку спрос на ИИ продолжает расти, возникает острая необходимость в разработке энергоэффективных алгоритмов и аппаратных средств для снижения воздействия вычислений ИИ на окружающую среду. Энергопотребление систем ИИ вызывает серьезную озабоченность, учитывая выбросы углекислого газа, связанные с невозобновляемыми источниками энергии (Rolnick et al., 2022).

Исследователи активно изучают методы повышения энергоэффективности алгоритмов ИИ. Например, сжатие моделей направлено на снижение вычислительных требований глубоких нейронных сетей за счет отсечения избыточных связей или уменьшения точности весов и активаций (Han et al., 2015). Такой подход позволяет существенно снизить энергопотребление и время вычислений без ущерба для производительности модели.

Другой подход – квантование, т. е. представление числовых значений меньшим количеством битов. Снижая точность параметров и активаций, квантование уменьшает объем памяти и сложность вычислений, что приводит к экономии энергии как при обучении, так и при использовании ИИ (Hubara et al., 2016). Также ведутся исследования по повышению энергоэффективности обучающих алгоритмов. Например, методы градиентного сжатия, такие как спарсификация и квантование, направлены на уменьшение коммуникационных затрат между распределенными устройствами в процессе обучения, что снижает энергопотребление (Alistarh et al., 2017). Кроме того, усовершенствование алгоритмов оптимизации и графиков скорости обучения позволяет минимизировать количество необходимых итераций, что приводит к экономии энергии (You et al., 2017).

Разработка энергоэффективного аппаратного обеспечения ИИ также является важным аспектом снижения энергопотребления. Традиционные вычислительные архитектуры часто не оптимизированы для рабочих нагрузок ИИ, что приводит к неэффективному использованию энергии. Для решения этой проблемы исследователи изучают новые аппаратные решения, включая нейроморфные вычисления и мемристоры, которые имитируют структуру и функционирование человеческого мозга, потенциально повышая энергоэффективность (Merolla et al., 2014; Prezioso et al., 2015).

8 European Commission. (n.d.). EU Climate Action. https://clck.ru/36kxSS

2. Образование электронных отходов

Помимо энергоемкости вычислений в системах ИИ, аппаратные средства, используемые в них, вызывают еще одну серьезную экологическую проблему – образование электронных отходов. Быстрое развитие технологий и постоянная потребность в более мощных аппаратных средствах приводят к их частой замене, а значит, к накоплению электронных отходов (Ferro et al., 2021).

Аппаратные средства ИИ, включая графические процессоры, интегральные схемы для приложений (ASIC) и другие специализированные компоненты, имеют относительно короткий срок службы в связи с неуклонным развитием технологий. По мере разработки новых поколений аппаратных средств старые быстро устаревают и часто выбрасываются, что обостряет проблему электронных отходов[9].

Неправильная утилизация аппаратных средств ИИ приводит к выбросу опасных веществ и материалов в окружающую среду. Эти вещества могут загрязнять почву, воду и воздух, создавая угрозу для экосистем и здоровья людей. Тем самым происходит не только ухудшение состояния окружающей среды, но и потеря ценных ресурсов, использованных в аппаратуре. Более того, утилизация аппаратуры, содержащей токсичные материалы, такие как свинец, ртуть и антипирены, может при неправильном обращении еще больше усугубить загрязнение окружающей среды[10].

Для решения проблемы образования электронных отходов очень важно внедрять экологически безопасные методы. Одним из подходов является содействие повторному использованию и переработке аппаратных средств ИИ. Реконструкция и восстановление старых аппаратных средств позволяют продлить срок их службы и сократить потребность в постоянном производстве новых устройств (Ferro et al., 2021). Кроме того, реализация программ приема оборудования и создание перерабатывающих предприятий могут обеспечить правильную утилизацию устройств и повторное использование ценных материалов[11].

При разработке и производстве аппаратных средств искусственного интеллекта следует руководствоваться принципами экологической безопасности. Использование материалов с меньшим воздействием на окружающую среду, возможность их вторичной переработки и уменьшение содержания вредных веществ могут способствовать достижению более устойчивого жизненного цикла аппаратных средств. Модульные конструкции, позволяющие заменять и модернизировать компоненты, также помогают продлить срок службы аппаратных средств ИИ и снизить частоту полной замены устройств (Ferro et al., 2021).

---

9 Baldé, C. P., Forti, V., Gray, V., Kuehr, R., &Stegmann, P. (2017). The global E-waste monitor 2017: Quantities, flows and resources. United Nations University, International Telecommunication Union, and International Solid Waste Association.

10 Там же.

11 Там же.

2.1. Быстрое развитие устройств с технологией искусственного интеллекта

Аппаратные технологии в области искусственного интеллекта стремительно развиваются, подпитываемые непрерывными инновациями, которые приводят к созданию все более мощных и эффективных систем (Amodei et al., 2016). Заметным событием в развитии аппаратных средств ИИ является превращение графических процессоров в ключевой компонент вычислений. Изначально задуманные для создания графических изображений, такие процессоры нашли широкое применение в ИИ благодаря своей способности эффективно решать задачи параллельной обработки данных (Amodei et al., 2016). Благодаря высокой пропускной способности и вычислительной мощности они хорошо подходят для обучения и внедрения моделей ИИ.

Кроме того, появились специализированные аппаратные средства ASIC, предназначенные для высоких рабочих нагрузок искусственного интеллекта. ASIC обеспечивают повышенную производительность и энергоэффективность за счет настройки аппаратной архитектуры для оптимизации выполнения алгоритмов ИИ (Amodei et al., 2016). Эти специализированные чипы обеспечивают более высокую плотность вычислений и скорость обработки данных по сравнению с процессорами общего назначения.

Стремительное развитие аппаратных средств сделало возможным совершение значительных прорывов в различных областях применения ИИ. Например, в области компьютерного зрения наличие высокопроизводительного оборудования позволило решать сложные задачи распознавания изображений и обнаружения объектов с поразительной точностью (Amodei et al., 2016). Аналогичным образом, в обработке естественного языка мощное оборудование ускоряет обучение и применение языковых моделей для решения таких задач, как машинный перевод и анализ эмоциональной окраски текста.

Однако стремительный прогресс в области аппаратных средств ИИ порождает и проблемы. Быстрая смена аппаратных средств в связи с появлением новых поколений приводит к значительному накоплению электронных отходов. Необходимо принимать меры по их утилизации и переработке, чтобы минимизировать воздействие на окружающую среду (Ferro et al., 2021).

Непрерывное появление новых аппаратных средств ИИ также создает трудности для разработчиков и исследователей. Чтобы оставаться в курсе новейших технологий, требуются постоянная адаптация, обучение и инвестиции, что создает проблемы для тех, кто занимается разработкой искусственного интеллекта (Amodei et al., 2016). Кроме того, оптимизация алгоритмов и программного обеспечения ИИ для использования возможностей различных аппаратных архитектур усложняет процесс разработки.

2.2. Жизненные циклы устройств и проблема электронных отходов

Стремительное развитие технологий искусственного интеллекта привело к росту числа электронных устройств, в результате чего увеличилось количество электронных отходов, представляющих значительную опасность для окружающей среды и здоровья людей[12]. Жизненный цикл аппаратных средств искусственного интеллекта играет решающую роль в определении объема образующихся электронных отходов и связанного с ними воздействия на окружающую среду.

[12] Там же.

Жизненный цикл аппаратных средств ИИ начинается с добычи сырья и процесса производства. Производство устройств искусственного интеллекта связано с добычей драгоценных металлов, редкоземельных элементов и других ценных материалов, многие из которых являются невозобновляемыми и требуют значительных затрат энергии (Ferro et al., 2021). Добыча и переработка этих материалов ухудшают состояние окружающей среды, а также часто связаны с использованием опасных веществ, которые могут нанести вред экосистемам и здоровью человека.

По мере быстрого развития аппаратных средств ИИ жизненный цикл устройств сокращается, и новые модели чаще приходят на смену старым. Это явление, известное как запланированное устаревание, усугубляет проблему электронных отходов, поскольку устаревшие устройства ИИ выбрасываются, что приводит к значительному накоплению электронных отходов[13]. Электронные отходы содержат опасные компоненты, такие как свинец, ртуть и антипирены, которые при неправильном обращении возвращаются в окружающую среду и загрязняют почву, водные источники и воздух.

Неправильная утилизация и неполноценная переработка электронных отходов еще больше усугубляют проблему. Многие электронные устройства попадают на свалки или сжигаются, выделяя токсичные вещества и способствуя загрязнению воздуха и почвы[14]. Неадекватная практика утилизации также приводит к потере ценных ресурсов, которые могли бы быть восстановлены и использованы повторно.

Необходимо на законодательном уровне разрабатывать нормативные акты и меры, способствующие надлежащему обращению с электронными отходами. Такие меры, как расширенная ответственность производителя, позволяют возложить на производителей ответственность за воздействие их продукции на окружающую среду в течение всего жизненного цикла, стимулируя их к внедрению экологически безопасных методов и инвестированию в инфраструктуру переработки[15]. Кроме того, разработка эффективных систем сбора, переработки и восстановления отходов будет способствовать повторному использованию устройств ИИ.

Перспективным решением проблемы электронных отходов является подход, основанный на циркулярной экономике. Она предполагает повторное использование, восстановление и переработку электронных устройств с целью минимизации потребления ресурсов и воздействия на окружающую среду (Ferro et al., 2021). Применяя принципы циркулярной экономики, можно разрабатывать аппаратные средства ИИ и управлять ими таким образом, чтобы максимально продлить срок их службы и снизить потребность в постоянном обновлении, тем самым уменьшая образование электронных отходов.

2.3. Стратегии ответственного обращения с электронными отходами в сфере искусственного интеллекта

Для решения экологических проблем, связанных с электронными отходами, образующимися при работе аппаратных средств ИИ, было предложено несколько стратегий, направленных на ответственное обращение с электронными отходами на протяжении

---

13 Baldé, C. P., Forti, V., Gray, V., Kuehr, R., &Stegmann, P. (2017). The global E-waste monitor 2017: Quantities, flows and resources. United Nations University, International Telecommunication Union, and International Solid Waste Association.

14 Там же.

15 Там же.

всего жизненного цикла устройств с искусственным интеллектом. Эти стратегии, направленные на смягчение негативных последствий утилизации электронных отходов и формирование более последовательного подхода к технологиям ИИ, включают:

1. Использование принципов «проектирование для демонтажа» (Design for Disassembly, DfD) и «проектирование для переработки» (Design for Recycling, DfR) при производстве аппаратных средств ИИ для эффективного разделения и переработки компонентов. Обеспечение простоты разборки и утилизации устройств позволяет сократить количество образующихся электронных отходов.

2. Применение концепции расширенной ответственности производителя. Она предусматривает ответственность производителей за весь жизненный цикл своей продукции, включая ее надлежащую утилизацию (Kahhat et al., 2008). Внедрение правил расширенной ответственности производителя применительно к аппаратным средствам искусственного интеллекта должно стимулировать производителей разрабатывать продукцию с учетом возможности ее переработки и брать на себя ответственность за ее экологически безопасные утилизацию и переработку.

3. Создание эффективных программ возврата и утилизации аппаратных средств искусственного интеллекта. Эта стратегия имеет решающее значение для обеспечения ответственной утилизации таких устройств. Производители могут сотрудничать со специализированными компаниями, занимающимися переработкой электронных отходов, или организовать пункты сбора, чтобы обеспечить надлежащую переработку таких устройств и предотвратить их попадание на свалки или в несанкционированные пункты утилизации.

4. Применение принципов циркулярной экономики. Эти принципы позволят минимизировать образование электронных отходов за счет повышения эффективности использования ресурсов и повторного применения продукции (Geissdoerfer et al., 2017). Такие стратегии, как восстановление и повторное использование аппаратных средств ИИ, а также создание вторичных рынков для бывших в употреблении устройств, продлевают срок службы систем искусственного интеллекта и снижают потребность в новом производстве.

5. Дальнейшие исследования в области передовых технологий утилизации для повышения эффективности переработки электронных отходов (Widmer et al., 2005). Такие инновации, как гидрометаллургические и биотехнологические процессы, позволяют извлекать ценные материалы из электронного оборудования, минимизируя при этом воздействие на окружающую среду и снижая зависимость от традиционных методов такого извлечения.

Реализация этих стратегий позволит внедрить в индустрию ИИ практику ответственного обращения с электронными отходами, что приведет к более устойчивому подходу к производству, использованию и утилизации аппаратных средств с искусственным интеллектом.

3. Инфраструктура центров обработки данных

В последние годы в связи с увеличением спроса на цифровые услуги наблюдается значительный рост центров обработки данных. Это привело к усилению их воздействия на окружающую среду. Строительство и эксплуатация центров обработки данных требуют значительных земельных и иных ресурсов, что приводит к изменению характера землепользования и разрушению окружающей среды (Mell & Grance, 2011). Кроме того, распространение центров обработки данных в городских районах вызывает опасения по поводу их влияния на местное население и инфраструктуру.

Центры обработки данных известны своим высоким энергопотреблением. Постоянная работа серверов, сетевого оборудования и систем охлаждения требует значительного количества электроэнергии. Охлаждение центров обработки данных представляет собой отдельную проблему. Тепло, выделяемое серверами и другим ИТ-оборудованием, требует эффективного отвода для поддержания оптимальных условий работы. Однако традиционные методы охлаждения, такие как кондиционирование воздуха, являются энергоемкими и неэффективными. Это побудило к поиску инновационных технологий охлаждения, включая жидкостное охлаждение и современные системы управления воздушными потоками, с целью повышения энергоэффективности и снижения воздействия центров обработки данных на окружающую среду (Masanet et al., 2020).

Вода является жизненно важным ресурсом, используемым в центрах обработки данных для охлаждения. Однако значительное потребление воды центрами обработки данных может привести к перегрузке местных водных ресурсов, особенно в регионах, где уже имеется нехватка воды или конкурирующий спрос на нее. Охлаждающие колонны, где происходит испарение, потребляют большие объемы воды.

Для решения проблемы воздействия центров обработки данных на окружающую среду заинтересованные стороны активно изучают и внедряют методы устойчивого развития. К таким практикам относятся:

1. Энергоэффективное проектирование. В центрах обработки данных могут применяться принципы энергоэффективного проектирования, такие как оптимизация загрузки серверов, совершенствование систем распределения электроэнергии и использование энергоэффективного оборудования. Эти меры позволяют существенно снизить энергопотребление и выбросы углекислого газа (Beloglazov et al., 2011).

2. Переход на возобновляемые источники энергии, такие как солнечная или ветровая энергия. Благодаря этому центры обработки данных могут снизить зависимость от ископаемого топлива и сократить выбросы парниковых газов.

3. Улавливание отработанного тепла и использование его в других целях, например, для отопления зданий или выработки электроэнергии. Такой подход позволяет максимально повысить энергоэффективность ЦОД и снизить их общее воздействие на окружающую среду.

4. Внедрение водосберегающих технологий охлаждения, таких как системы охлаждения с замкнутым циклом и водосберегающие охлаждающие колонны. Это позволяет снизить потребление воды в ЦОД. Кроме того, рециркуляция и повторное использование воды могут снизить нагрузку на местные водные ресурсы.

С помощью этих методов можно сбалансировать растущий спрос на цифровые услуги с минимизацией воздействия на окружающую среду, способствуя созданию более устойчивой и ответственной цифровой инфраструктуры.

4. Понятие предвзятости данных при обучении искусственного интеллекта

С целью принятия обоснованных решений алгоритмы искусственного интеллекта в значительной степени опираются на обучающие данные. Однако базы данных могут быть предвзятыми, приводя к необъективным результатам при принятии экологических решений. Предвзятость обучающих данных может возникать по различным причинам. Например, данные могут отражать существующее социальное

неравенство и системные предубеждения (Caliskan et al., 2017). Для обеспечения справедливого и равноправного процесса принятия экологических решений крайне важно распознавать и устранять эти предубеждения.

Предвзятость приложений с ИИ в процессе принятия экологических решений может усугубить дисбаланс в области охраны окружающей среды, с которым сталкиваются маргинализированные сообщества. Например, если алгоритмы искусственного интеллекта обучаются на наборах данных, непропорционально представляющих благополучные районы, то при принятии решений о распределении ресурсов или экологической политике могут игнорироваться потребности и проблемы маргинализированных сообществ (Benjamin, 2019). Тем самым эти сообщества еще больше маргинализируются, экологическая несправедливость закрепляется.

Необъективные приложения ИИ могут закреплять и усиливать неравенство, усугубляя существующие социальные, экономические и экологические диспропорции. Например, если алгоритмы искусственного интеллекта предвзято относятся к определенным демографическим группам или географическим районам, это может привести к неравному распределению экологических благ, таких как доступ к чистому воздуху, воде или зеленым насаждениям. Кроме того, необъективные алгоритмы могут привести к дискриминационным результатам, таким как непропорциональное бремя загрязнения или недостаточная защита окружающей среды в маргинализированных сообществах.

Для устранения предвзятости и обеспечения справедливости при принятии решений в области экологии с помощью искусственного интеллекта необходимо принять ряд мер:

1. Важно обеспечить, чтобы базы данных для обучения ИИ охватывали различные точки зрения и корректно отражали соответствующие сообщества. Для этого необходимо тщательно следить за отбором данных, чтобы не допустить недостатков в представлении данных и усиления существующих предубеждений (Sweeney, 2013).

2. Разработка прозрачных и понятных алгоритмов ИИ позволяет тщательно изучить их и выявить возможную предвзятость. Тем самым все заинтересованные стороны, в том числе соответствующие сообщества, могут понять, как принимаются решения, и бороться с потенциальными предубеждениями (Burrell, 2016).

3. Непрерывный мониторинг и оценка систем ИИ крайне важны для выявления и устранения предвзятости, которая может проявиться с течением времени. Это предполагает постоянную оценку воздействия приложений ИИ на различные группы населения и их соответствие целям равенства и справедливости (Crawford & Calo, 2016).

4. Привлечение соответствующих сообществ к разработке, внедрению и оценке процессов принятия экологических решений с использованием искусственного интеллекта может способствовать обеспечению справедливости и равноправия.

Устранение предвзятости в базах данных для обучения ИИ, признание экологического неравенства, с которым сталкиваются маргинализированные сообщества, и реализация мер по обеспечению справедливости и равноправия позволяют снизить риск усиления экологической несправедливости, вызванный применением искусственного интеллекта. Приложения ИИ, функционирующие на принципах ответственности и инклюзии, должны поддерживать процессы принятия обоснованных и справедливых решений и способствовать формированию более справедливой и устойчивой окружающей среды для всех.

5. Разрушение природных экосистем

Развитие технологий искусственного интеллекта и их интеграция в различные отрасли экономики вызывают опасения относительно их потенциального воздействия на природные экосистемы. Одной из проблем является нарушение среды обитания и миграционных процессов диких животных. Инфраструктура, создаваемая для функционирования ИИ, например, центры обработки данных и коммуникационные сети, часто требует значительного использования земли, что приводит к фрагментации и разрушению среды обитания. Это негативно сказывается на популяциях диких животных, ограничивая их доступ к ресурсам и нарушая важнейшие пути миграции, что в конечном итоге создает угрозу биоразнообразию и экологической устойчивости.

Использование ИИ для экологического мониторинга и охраны окружающей среды открывает широкие возможности, но и создает проблемы. С одной стороны, искусственный интеллект позволяет эффективно собирать, анализировать и интерпретировать данные, тем самым улучшая наше понимание биоразнообразия, изменения климата и состояния экосистем. Он дает возможность выявлять закономерности, делать прогнозы и обосновывать стратегии сохранения окружающей среды. С другой стороны, если чрезмерно полагаться на ИИ, сократить полевые исследования и участие человека, то можно упустить важные нюансы экологических процессов, заметные только при непосредственном наблюдении (Koh & Wich, 2012).

Чтобы уменьшить экологические последствия использования ИИ, необходимо применять ответственные методы его внедрения. Они включают в себя проведение комплексной оценки воздействия на окружающую среду перед внедрением технологий ИИ, оценку потенциальных рисков для экосистем и определение соответствующих стратегий по их снижению. Кроме того, важно интегрировать искусственный интеллект в существующие природоохранные стратегии и привлекать местное население к процессу принятия решений. Такой комплексный подход будет способствовать целостному пониманию экологических систем и созданию приложений ИИ на пользу как биоразнообразию, так и благополучию человека.

6. Действующее законодательство ЕС в области воздействия искусственного интеллекта на окружающую среду

Развитие искусственного интеллекта побудило правительства и регулирующие органы разных стран обратить внимание на его потенциальное воздействие на окружающую среду. Некоторые страны и регионы уже предприняли шаги по регулированию экологических издержек от применения искусственного интеллекта.

В Европейском союзе с марта 2020 г. действует Директива EcoDesign (2009/125/EC) о работе серверов и устройств хранения данных. Эта норма устанавливает минимальные требования к энергоэффективности этих продуктов, в том числе и тех, которые используются в аппаратных средствах искусственного интеллекта. Она направлена на снижение энергопотребления и уменьшение воздействия на окружающую среду центров обработки данных и других компонентов инфраструктуры ИИ[16].

[16] Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products (recast) (Text with EEA relevance). Official Journal of the European Union, L 285, 10–35. https://clck.ru/36kxU5

Наряду с Директивой EcoDesign важнейшую роль в рациональном использовании электронных отходов, включая аппаратные компоненты ИИ, играет Директива об отработанном электрическом и электронном оборудовании (Waste Electrical and Electronic Equipment, WEEE). Директива WEEE устанавливает правила надлежащего обращения и утилизации электронных отходов, обеспечивая экологически ответственное обращение с отработанным аппаратным обеспечением ИИ. Ответственность за сбор и переработку электронных отходов возлагается на производителей и пользователей, что способствует развитию циркулярной экономики и минимизации воздействия на окружающую среду при утилизации аппаратных средств искусственного интеллекта[17].

В рамках оценки Директивы WEEE на июнь 2023 г. была запланирована общественная консультация, позволяющая всем заинтересованным сторонам и широкой общественности высказать свои замечания и мнения по поводу эффективности и возможных усовершенствований этой Директивы.

В марте 2020 г. в Европейском союзе также вступил в силу Регламент (EU) 2019/424 о требованиях к экологическому дизайну серверов и устройств хранения данных. Данный регламент устанавливает минимальные требования к энергоэффективности этих продуктов, в том числе используемых в аппаратных средствах ИИ, с целью снижения энергопотребления и уменьшения воздействия на окружающую среду центров обработки данных и других компонентов инфраструктуры искусственного интеллекта[18].

Эти нормативные акты Европейского союза свидетельствуют о стремлении решить проблему воздействия искусственного интеллекта на окружающую среду и содействовать внедрению экологически безопасных практик в технологический сектор. Устанавливая стандарты энергоэффективности и стимулируя ответственное обращение с электронными отходами, ЕС преследует цель содействовать более экологичному и безопасному для окружающей среды подходу к разработке и внедрению искусственного интеллекта.

Заключение

Итак, рассмотрев скрытые экологические издержки, связанные с искусственным интеллектом, следует отметить, что мы должны признать и устранить возможные экологические последствия его развития и внедрения. Энергоемкость вычислений ИИ, образование электронных отходов, нарушение природных экосистем, возможность принятия необъективных решений – все это указывает на необходимость принятия упреждающих мер. Признавая значение практик устойчивого развития, таких как энергоэффективные алгоритмы, переход на возобновляемые источники энергии, ответственное обращение с электронными отходами и этические аспекты, мы стремимся к более гармоничному и экологичному использованию искусственного интеллекта.

---

17 Consolidated text: Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) (Text with EEA relevance). https://clck.ru/36kxYS

18 Commission Regulation (EU) 2019/424 of 15 March 2019 laying down ecodesign requirements for servers and data storage products pursuant to Directive 2009/125/EC of the European Parliament and of the Council and amending Commission Regulation (EU) No 617/2013 (Text with EEA relevance). Official Journal of the European Union, L 74, 46–66. https://clck.ru/36kxbm

Мы все вместе несем ответственность за то, чтобы проложить путь к лучшему будущему, в котором искусственный интеллект принесет пользу и человечеству, и планете. Уделяя первостепенное внимание экологической устойчивости и предпринимая активные шаги по снижению экологического следа ИИ, мы сможем создать будущее, в котором его потенциал будет служить сохранению и защите наших природных ресурсов. Благодаря сотрудничеству, исследованиям, разработке государственных мер и нормативных актов мы сможем направить развитие искусственного интеллекта в более устойчивое и этически верное русло.

Список литературы

Alistarh, D., Grubic, D., Li, J., Tomioka, R., & Vojnovic, M. (2017). QSGD: Communication-efficient SGD via gradient quantization and encoding. *Advances in neural information processing systems*, *30*. https://doi.org/10.48550/arXiv.1610.02132

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety*. https://doi.org/10.48550/arXiv.1606.06565

Beloglazov, A., Buyya, R., Lee, Y. C., & Zomaya, A. (2011). A taxonomy and survey of energy-efficient data centers and cloud computing systems. *Advances in computers*, *82*, 47–111. https://doi.org/10.1016/B978-0-12-385512-1.00003-7

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Cambridge: Polity.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, *356*(6334), 183–186. https://doi.org/10.1126/science.aal4230

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

Dhar, P. (2020). The carbon impact of artificial intelligence. *Nat. Mach. Intell.*, *2*(8), 423–425. https://doi.org/10.1038/s42256-020-0219-9

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics*, *10*(13), 1539. https://doi.org/10.3390/electronics10131539

Ferro, M., Silva, G. D., de Paula, F. B., Vieira, V., & Schulze, B. (2021). Towards a sustainable artificial intelligence: A case study of energy efficiency in decision tree algorithms. *Concurrency and Computation: Practice and Experience*, *e6815*. https://doi.org/10.1002/cpe.6815

Geissdoerfer, M., Savaget, P., Bocken, N. M., & Hultink, E. J. (2017). The Circular Economy–A new sustainability paradigm? *Journal of cleaner production*, *143*, 757–768. https://doi.org/10.1016/j.jclepro.2016.12.048

Han, S., Pool, J., Tran, J., & Dally, W. (2015). Learning both weights and connections for efficient neural network. In *Advances in neural information processing systems 28*. https://doi.org/10.48550/arXiv.1506.02626

Hanus, N., Newkirk, A., & Stratton, H. (2023). Organizational and psychological measures for data center energy efficiency: barriers and mitigation strategies. *Energy Efficiency*, *16*(1), 1–18. https://doi.org/10.1007/s12053-022-10078-1

Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., & Meger, D. (2018). Deep reinforcement learning that matters. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 32, No. 1). https://doi.org/10.1609/aaai.v32i1.11694

Hubara, I., Courbariaux, M., Soudry, D., El-Yaniv, R., & Bengio, Y. (2016). Quantized neural networks: Training neural networks with low precision weights and activations. *The Journal of Machine Learning Research*, *18*(1), 6869–6898. https://doi.org/10.48550/arXiv.1609.07061

Kahhat, R., Kim, J., Xu, M., Allenby, B., Williams, E., & Zhang, P. (2008). Exploring e-waste management systems in the United States. *Resources, conservation and recycling*, *52*(7), 955–964. https://doi.org/10.1016/j.resconrec.2008.03.002

Koh, L. P., & Wich, S. A. (2012). Dawn of drone ecology: low-cost autonomous aerial vehicles for conservation. *Tropical conservation science*, *5*(2), 121–132. https://doi.org/10.1177/194008291200500202

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-145

Merolla, P. A., Arthur, J. V., Alvarez-Icaza, R., Cassidy, A. S., Sawada, J., Akopyan, F., ... & Modha, D. S. (2014). A million spiking-neuron integrated circuit with a scalable communication network and interface. *Science*, *345*(6197), 668–673. https://doi.org/10.1126/science.1254642

Prezioso, M., Merrikh-Bayat, F., Hoskins, B. D., Adam, G. C., Likharev, K. K., & Strukov, D. B. (2015). Training and operation of an integrated neuromorphic network based on metal-oxide memristors. *Nature*, *521*(7550), 61–64. https://doi.org/10.1038/nature14441

Ram, M., Child, M., Aghahosseini, A., Bogdanov, D., Lohrmann, A., & Breyer, C. (2018). A comparative analysis of electricity generation costs from renewable, fossil fuel and nuclear sources in G20 countries for the period 2015-2030. *Journal of Cleaner Production*, *199*, 687–704. https://doi.org/10.1016/j.jclepro.2018.07.159

Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling climate change with machine learning. *ACM Computing Surveys (CSUR)*, *55*(2), 1–96. https://doi.org/10.1145/3485128

Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2020). Green AI. *Communications of the ACM*, *63*(12), 54–63. https://doi.org/10.1145/3381831

Şerban, A. C., & Lytras, M. D. (2020). Artificial intelligence for smart renewable energy sector in Europe – smart energy infrastructures for next generation smart cities. *IEEE access*, *8*, 77364–77377. https://doi.org/10.1109/ACCESS.2020.2990123

Shah, A., Bash, C., Sharma, R., Christian, T., Watson, B. J., & Patel, C. (2010). The environmental footprint of data centers. In *ASME 2009 InterPACK Conference* (Vol. 2, pp. 653-662).San Francisco, CA. https://doi.org/10.1115/InterPACK2009-89036

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. https://doi.org/10.48550/arXiv.1906.02243

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, *56*(5), 44–54. https://doi.org/10.1145/2447976.2447990

Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., Schnellmann, M., & Böni, H. (2005). Global perspectives on e-waste. *Environmental Impact Assessment Review*, *25*(5), 436–458. https://doi.org/10.1016/j.eiar.2005.04.001

You, Y., Gitman, I., & Ginsburg, B. (2017). *Large batch training of convolutional networks*. https://doi.org/10.48550/arXiv.1708.03888

Сведения об авторе

Алеся Жук – соискатель степени PhD, факультет права и философии, Университет Помпеу Фабра; ассистент преподавателя, Барселонский институт международных исследований
Адрес: 08005, Испания, Барселона, Рамон Триас Фаргас, 25-27
E-mail: alesia.zhuk@ug.uchile.cl
ORCID ID: https://orcid.org/0000-0002-6295-6839
Google Scholar ID: https://scholar.google.com/citations?user=PVCH_B0AAAAJ

Конфликт интересов

Автор сообщает 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: 10.53.91 / Экологическое право в отдельных странах
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 29 июня 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.40

Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues

Alesia Zhuk

University Pompeu Fabra
Barcelona, Spain

Keywords

algorithmic bias,
artificial intelligence,
data center,
digital technologies,
ecological costs,
electronic waste,
energy consumption,
law,
natural ecosystems,
sustainability

Abstract

Objective: to identify the hidden ecological costs associated with the elaboration, implementation and development of artificial intelligence technologies, in order to ensure its sustainable and harmonious integration with various economic sectors by identifying optimal moral-ethical and political-legal strategies.

Methods: the conducted research is based on an ecological approach to the development and implementation of artificial intelligence, as well as on an interdisciplinary and political-legal analysis of ecological problems and risks of algorithmic bias, errors in artificial intelligence algorithms and decision-making processes that may exacerbate environmental inequalities and injustice towards the environment. In addition, analysis was performed in regard to the consequences of natural ecosystems destruction caused by the development of artificial intelligence technologies due to the computing energy-intensiveness, the growing impact of data centers on energy consumption and problems with their cooling, the electronic waste formation due to the rapid improvement of equipment, etc.

Results: the analysis shows a range of environmental, ethical and political-legal issues associated with the training, use and development of artificial intelligence, which consumes a significant amount of energy (mainly from non-renewable sources). This leads to an increase in carbon emissions and creates obstacles to further sustainable ecological development. Improper disposal of artificial intelligence equipment exacerbates the problem of e-waste and pollution of the planet, further damaging the environment.

Errors in artificial intelligence algorithms and decision-making processes lead to environmental injustice and inequality. AI technologies may disrupt natural ecosystems, jeopardizing wildlife habitats and migration patterns.

Scientific novelty: the environmental consequences of the artificial intelligence use and further development, as well as the resulting environmental violations and costs of sustainable development, were studied. This leads to the scientific search for optimal strategies to minimize environmental damage, in which legal scholars and lawyers will have to determine ethical-legal and political-legal solutions at the national and supranational levels.

Practical significance: understanding the environmental impact of AI is crucial for policy makers, lawyers, researchers, and industry experts in developing strategies to minimize environmental harm. The findings emphasize the importance of implementing energy efficient algorithms, switching to renewable energy sources, adopting responsible e-waste management practices, ensuring fairness in AI decision-making and taking into account ethical considerations and rules of its implementation.

For citation

Zhuk, A. (2023). Artificial Intelligence Impact on the Environment: Hidden Ecological Costs and Ethical-Legal Issues. *Journal of Digital Technologies and Law, 1*(4), 932–954. https://doi.org/10.21202/jdtl.2023.40

References

Alistarh, D., Grubic, D., Li, J., Tomioka, R., & Vojnovic, M. (2017). QSGD: Communication-efficient SGD via gradient quantization and encoding. *Advances in neural information processing systems*, *30*. https://doi.org/10.48550/arXiv.1610.02132

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). *Concrete problems in AI safety*. https://doi.org/10.48550/arXiv.1606.06565

Beloglazov, A., Buyya, R., Lee, Y. C., & Zomaya, A. (2011). A taxonomy and survey of energy-efficient data centers and cloud computing systems. *Advances in computers*, *82*, 47–111. https://doi.org/10.1016/B978-0-12-385512-1.00003-7

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Cambridge: Polity.

Burrell, J. (2016). How the machine 'thinks': Understanding opacity in machine learning algorithms. *Big Data & Society*, *3*(1). https://doi.org/10.1177/2053951715622512

Caliskan, A., Bryson, J. J., & Narayanan, A. (2017). Semantics derived automatically from language corpora contain human-like biases. *Science*, *356*(6334), 183–186. https://doi.org/10.1126/science.aal4230

Crawford, K., & Calo, R. (2016). There is a blind spot in AI research. *Nature*, *538*(7625), 311–313. https://doi.org/10.1038/538311a

Dhar, P. (2020). The carbon impact of artificial intelligence. *Nat. Mach. Intell.*, *2*(8), 423–425. https://doi.org/10.1038/s42256-020-0219-9

Ding, Q., Zhu, R., Liu, H., & Ma, M. (2021). An overview of machine learning-based energy-efficient routing algorithms in wireless sensor networks. *Electronics*, *10*(13), 1539. https://doi.org/10.3390/electronics10131539

Ferro, M., Silva, G. D., de Paula, F. B., Vieira, V., & Schulze, B. (2021). Towards a sustainable artificial intelligence: A case study of energy efficiency in decision tree algorithms. *Concurrency and Computation: Practice and Experience*, *e6815*. https://doi.org/10.1002/cpe.6815

Geissdoerfer, M., Savaget, P., Bocken, N. M., & Hultink, E. J. (2017). The Circular Economy–A new sustainability paradigm? *Journal of cleaner production*, *143*, 757–768. https://doi.org/10.1016/j.jclepro.2016.12.048

Han, S., Pool, J., Tran, J., & Dally, W. (2015). Learning both weights and connections for efficient neural network. In *Advances in neural information processing systems 28*. https://doi.org/10.48550/arXiv.1506.02626

Hanus, N., Newkirk, A., & Stratton, H. (2023). Organizational and psychological measures for data center energy efficiency: barriers and mitigation strategies. *Energy Efficiency*, *16*(1), 1–18. https://doi.org/10.1007/s12053-022-10078-1

Henderson, P., Islam, R., Bachman, P., Pineau, J., Precup, D., & Meger, D. (2018). Deep reinforcement learning that matters. In *Proceedings of the AAAI conference on artificial intelligence* (Vol. 32, No. 1). https://doi.org/10.1609/aaai.v32i1.11694

Hubara, I., Courbariaux, M., Soudry, D., El-Yaniv, R., & Bengio, Y. (2016). Quantized neural networks: Training neural networks with low precision weights and activations. *The Journal of Machine Learning Research*, *18*(1), 6869–6898. https://doi.org/10.48550/arXiv.1609.07061

Kahhat, R., Kim, J., Xu, M., Allenby, B., Williams, E., & Zhang, P. (2008). Exploring e-waste management systems in the United States. *Resources, conservation and recycling*, *52*(7), 955–964. https://doi.org/10.1016/j.resconrec.2008.03.002

Koh, L. P., & Wich, S. A. (2012). Dawn of drone ecology: low-cost autonomous aerial vehicles for conservation. *Tropical conservation science*, *5*(2), 121–132. https://doi.org/10.1177/194008291200500202

Masanet, E., Shehabi, A., Lei, N., Smith, S., & Koomey, J. (2020). Recalibrating global data center energy-use estimates. *Science*, *367*(6481), 984–986. https://doi.org/10.1126/science.aba3758

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-145

Merolla, P. A., Arthur, J. V., Alvarez-Icaza, R., Cassidy, A. S., Sawada, J., Akopyan, F., ... & Modha, D. S. (2014). A million spiking-neuron integrated circuit with a scalable communication network and interface. *Science*, *345*(6197), 668–673. https://doi.org/10.1126/science.1254642

Prezioso, M., Merrikh-Bayat, F., Hoskins, B. D., Adam, G. C., Likharev, K. K., & Strukov, D. B. (2015). Training and operation of an integrated neuromorphic network based on metal-oxide memristors. *Nature*, *521*(7550), 61–64. https://doi.org/10.1038/nature14441

Ram, M., Child, M., Aghahosseini, A., Bogdanov, D., Lohrmann, A., & Breyer, C. (2018). A comparative analysis of electricity generation costs from renewable, fossil fuel and nuclear sources in G20 countries for the period 2015-2030. *Journal of Cleaner Production*, *199*, 687–704. https://doi.org/10.1016/j.jclepro.2018.07.159

Rolnick, D., Donti, P. L., Kaack, L. H., Kochanski, K., Lacoste, A., Sankaran, K., ... & Bengio, Y. (2022). Tackling climate change with machine learning. *ACM Computing Surveys (CSUR)*, *55*(2), 1–96. https://doi.org/10.1145/3485128

Schwartz, R., Dodge, J., Smith, N. A., & Etzioni, O. (2020). Green AI. *Communications of the ACM*, *63*(12), 54–63. https://doi.org/10.1145/3381831

Şerban, A. C., & Lytras, M. D. (2020). Artificial intelligence for smart renewable energy sector in Europe – smart energy infrastructures for next generation smart cities. *IEEE access*, *8*, 77364–77377. https://doi.org/10.1109/ACCESS.2020.2990123

Shah, A., Bash, C., Sharma, R., Christian, T., Watson, B. J., & Patel, C. (2010). The environmental footprint of data centers. In *ASME 2009 InterPACK Conference* (Vol. 2, pp. 653–662). San Francisco, CA. https://doi.org/10.1115/InterPACK2009-89036

Strubell, E., Ganesh, A., & McCallum, A. (2019). Energy and policy considerations for deep learning in NLP. https://doi.org/10.48550/arXiv.1906.02243

Sweeney, L. (2013). Discrimination in online ad delivery. *Communications of the ACM*, *56*(5), 44–54. https://doi.org/10.1145/2447976.2447990

Widmer, R., Oswald-Krapf, H., Sinha-Khetriwal, D., Schnellmann, M., & Böni, H. (2005). Global perspectives on e-waste. *Environmental Impact Assessment Review*, *25*(5), 436–458. https://doi.org/10.1016/j.eiar.2005.04.001

You, Y., Gitman, I., & Ginsburg, B. (2017). *Large batch training of convolutional networks*. https://doi.org/10.48550/arXiv.1708.03888

Author information

Alesia Zhuk – PhD Candidate, Law and Philosophy Group at Universitat Pompeu Fabra, Teaching Assistant, Institut Barcelona d'Estudis Internacionals
Address: Ramon Trias Fargas, 25-27. 08005 Barcelona, Spain
E-mail: alesia.zhuk@ug.uchile.cl
ORCID ID: https://orcid.org/0000-0002-6295-6839
Google Scholar ID: https://scholar.google.com/citations?user=PVCH_B0AAAAJ

Conflicts of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – June 29, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:17:296.41:004.8
EDN: https://elibrary.ru/mdiefv
DOI: https://doi.org/10.21202/jdtl.2023.41

Этика искусственного интеллекта и робототехники: ключевые проблемы и современные способы их решения

Нидика Ядав

Независимый исследователь
г. Нью-Дели, Индия

Ключевые слова

ChatGPT,
безопасность,
искусственный интеллект,
кибербезопасность,
конфиденциальность данных,
право,
робот,
робототехника,
цифровые технологии,
этика

Аннотация

Цель: современные достижения в области развития и распространения цифровых технологий привлекли внимание ученых и практиков к обсуждению ключевых этических проблем, связанных с искусственным интеллектом и робототехникой, в связи с чем в настоящем исследовании представлены результаты этой дискуссии и обозначены наиболее актуальные задачи, решение которых определяет пути совершенствования регулирования искусственного интеллекта и робототехники в части морализации технологий.

Методы: в процессе исследования использовались практико- и риск-ориентированный подходы, дополняемые мультидисциплинарным анализом документов (европейских принципов и кодексов этики) и исследований, в том числе посвященных различным проблемам искусственного интеллекта и робототехники.

Результаты: в статье обозначены ключевые этические проблемы в области искусственного интеллекта и робототехники; установлено, что затрагиваемые ключевые этические проблемы могут быть решены при условии, если они получат юридическое оформление и будут реализованы на международном уровне; предложенный автором алгоритм, основанный на анализе практики применения цифровых технологий, позволит усовершенствовать нравственные действия технологий при принятии ими решений.

Научная новизна: в данной статье представлены новейшие этические проблемы, которые волнуют ученых и практиков в области искусственного интеллекта и робототехники, и методы их решения этико-правовыми средствами, направленными на морализацию технологий и повышение ее ответственности.

Практическая значимость: все решения, представленные в статье, имеют практическое значение и готовы к широкому внедрению на международном уровне. Их оформление в нормативном виде и последующее соблюдение приведут к уменьшению вреда, который может нанести искусственный интеллект в прикладных областях, в том числе в робототехнике с использованием искусственного интеллекта. В связи с этим нормативные, в том числе законодательные, решения должны быть приняты как можно скорее, чтобы искусственный интеллект и робототехника приобрели статус надежных инструментов при использовании этих систем на работе, дома и в других сферах, таких как торговые центры, магазины, школы, университеты и т. д.

Для цитирования

Ядав, Н. (2023). Этика искусственного интеллекта и робототехники: ключевые проблемы и современные способы их решения. *Journal of Digital Technologies and Law*, *1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

Содержание

Введение

Технология искусственного интеллекта (далее – ИИ) (Rich et al., 2009) в последнее время набирает все большие обороты. За последние несколько лет достигнут колоссальный прогресс в каждой из областей применения ИИ (Saveliev et al., 2021). Более того, многие аспекты последних разработок в области ИИ нельзя было и представить (Xiao-Fan et al., 2023; Kumar et al., 2023). Так, даже сами создатели такого ИИ-продукта, как ChatGPT, были ошеломлены тем, каких вершин развития они достигли.

Это лишь один из примеров; прогресс наблюдается не только в генерации текстов, но и во многих областях исследований ИИ. Некоторые из них мы рассмотрим в данной статье.

Термин «искусственный интеллект» был введен для обозначения технологии, которая имитирует работу человеческого мозга для выполнения сложных человеческих действий. При этом преследуется цель облегчить труд человеческий, производя его так же, как это делает человек, или оказывать помощь в решении задач, поставленных перед ним. Предмет ИИ (Rich et al., 2009; Stahl, 2021; Mueller, 2012) представляет собой объединение многих областей, таких как информатика, математика, когнитивные науки, психология и др. ИИ зародился в начале 50-х годов прошлого века и с тех пор привлекает внимание исследователей (Turing, 2009; Schank, 1991). Эта тема разрабатывалась с целью создания алгоритмов и/или машин, которые могли бы выполнять работу или действовать подобно человеку, а в некоторых случаях, когда человек не мог выполнять работу, интеллектуальные машины на основе ИИ могли бы заменить его, например при добыче минералов в земной коре (Lesandrini et al., 2023; Memarian & Doleck, 2023).

Перед ИИ никогда не ставилась цель причинить вред людям, заменить человека или захватить мир людей. Цель ИИ – дополнить человека, помочь людям совершать научные открытия или бороться с природными катаклизмами, помочь человеку в таких ситуациях, как пандемия и т. д. Другие области применения, в которых ИИ, как представляется, может быть полезным людям, – это повседневная медицинская помощь, работа в машиностроительных компаниях, управление полуавтоматическими и полностью автоматизированными автомобилями, доставка грузов с помощью ботов в чрезвычайных ситуациях, например, при наводнениях. Интеллектуальная робототехника может найти применение в самых разных областях, от текстильной промышленности до управления самолетами, от организации дорожного движения до космических программ и т. д.

В настоящее время развитие искусственного интеллекта достигло больших высот, и он может выполнять работу, которую делает человек, практически во всех областях. Искусственный интеллект заменяет множество рабочих мест, но это не должно пугать людей. Новые рабочие места появляются с той же скоростью, однако статистика создания новых рабочих мест на месте исчезнувших не сразу становится известной простым людям. Именно так шло развитие со времен промышленной революции. Да, освоить новую сферу деятельности из-за того, что искусственный интеллект отменил многие рабочие процессы, не так-то просто. Все мы помним, как в результате компьютеризации текстильного производства было ликвидировано множество рабочих мест. Пострадавшим инженерам пришлось искать новую работу. Как только какая-то область устаревает, начинается развитие новой области. Так, с появлением мобильных телефонов стали неактуальными стационарные телефоны. Сегодня те же мобильные телефоны обеспечивают работой множество людей по всему миру. Подробнее о решении проблемы потери рабочих мест будет рассказано в следующих разделах.

Цель данной статьи – рассказать об этических аспектах искусственного интеллекта, его этическом использовании и предложить пути решения проблем, возникающих в связи с развитием ИИ и особенно комбинации ИИ с робототехникой. В разделе 2 описаны причины, побудившие к изучению этических проблем ИИ и робототехники. В разделе 3 рассматриваются вопросы использования ИИ в робототехнике. В разделе 4 предложены решения основных этических проблем в области ИИ и робототехники, а в разделе 5 даны выводы по работе.

1. Общая информация об этике искусственного интеллекта и робототехники

Несмотря на множество полезных применений искусственного интеллекта, многие воспринимают его как угрозу. Однако, как и в других областях науки, ИИ представляет самостоятельный предмет изучения. В данной статье рассматривается необходимость установления этических норм в ИИ и робототехнике. Следует знать, что, как и в случае других наук, необходимо иметь представление об определенных ограничениях при разработке, открытии и внедрении искусственного интеллекта. В этом нет ничего нового, такие хорошо развитые дисциплины, как химия, физика, биология и другие, имеют свои правила использования. Примером может служить утечка выращенных в лаборатории грибков, которые могут создать хаос в природе. Это может произойти в результате отсутствия должного внимания и несоблюдения протоколов лаборатории, в которой грибки хранились для проведения практических работ. Таким образом, во всех областях науки существуют меры защиты; они должны применяться и в области искусственного интеллекта и робототехники. Другой пример – новый автомобиль, в котором для работы двигателей используется ядерная энергия. Если его не протестировать в экстремальных температурных условиях, это может привести к многочисленным проблемам.

Разница между другими научными дисциплинами и ИИ заключается в том, что ИИ вырос из ряда научных дисциплин, в основном информатики и математики, в которых не существует протоколов выпуска результатов. Таким образом, выпуск продуктов ИИ начался без научных и социальных рекомендаций по их внедрению. Другая причина заключается в том, что ИИ все еще является новшеством по сравнению с другими дисциплинами, и это необходимо учитывать при определении ограничений на производство устройств с искусственным интеллектом.

К счастью, серьезных регулярных сбоев в работе искусственного интеллекта и робототехники пока не наблюдается. Некоторое время назад возник ряд проблем, касавшихся автономных автомобилей и системы рекомендательных норм одного из технологических гигантов. В будущем появится еще больше продуктов ИИ и робототехники, но они должны быть этичными, поскольку на них лежит большая ответственность. ИИ помог человеку достичь того уровня развития, который существует сегодня. В той или иной мере искусственным интеллектом оснащены многие устройства и продукты, которыми мы пользуемся, от стиральной и посудомоечной машины до онлайн-бронирования билетов на отдых. Все это будет использоваться и в будущем. Развитие ИИ невозможно остановить, поэтому для более полного раскрытия потенциала ИИ и робототехники необходимо соблюдать этические нормы.

Сейчас ИИ является самостоятельным объектом. Необходимо выработать специальные инструкции для ИИ. Как физические эксперименты проводятся согласно заранее определенным инструкциям, так и все эксперименты в области ИИ и робототехники должны следовать установленным инструкциям. Это должно быть сделано для каждого приложения ИИ. Составление инструкций может занять некоторое время, но это необходимо, поскольку правила будут определяться на научной основе. Соответствие правилам должно проверяться до выпуска на рынок каждого продукта ИИ, будь то робототехника или простая программа (Rich et al., 2009), запускающая песню, исходя из ваших предпочтений. Таким образом, необходимо установить соответствующие правила для всех разработчиков ИИ.

2. Робототехника

Понятие «робототехника» очень обширное и до сих пор достаточно размытое. Как правило, роботы определяются как устройства, которые способны совершать механические движения и могут быть как с искусственным интеллектом, так и без него. Соответственно, робототехника – это дисциплина, изучающая роботов (Agarwal & Stoff, 2023). Однако в данной статье речь пойдет об интеллектуальных роботах (Joachim et al., 2021), которые могут управляться и работать на основе искусственного интеллекта. В сфере робототехники применяются как простые механические роботы, так и роботы для медицинской хирургии, и даже гуманоидные роботы, способные к самостоятельным исследованиям и полетам в космос, но при этом так или иначе управляемые человеком.

Есть и другие проблемы с определением понятия «робот» как машины с дистанционным управлением для выполнения тех или иных задач. По этому поводу также ведутся дискуссии (De Felice et al., 2022), называть ли такое устройство интеллектуальным роботом. На этот вопрос отвечают по-разному, но мы считаем, что такая машина является интеллектуальным роботом, поскольку она управляется не человеческим мозгом, а сигналами, посылаемыми на расстоянии через Интернет или другие источники. Примером таких устройств являются, например, боты на базе интернета вещей. Тем самым определение робототехники, причем именно интеллектуальной робототехники, расширяется. Они имитируют работу мозга, хотя и посредством канала связи. Таким образом, законы этики в робототехнике распространяются и на все подобные устройства.

Почему анализ робототехники важен при обсуждении этики ИИ? Причина этого в том, что робототехника – это будущее, к которому движется ИИ. Роботы всегда должны контролироваться и изменяться людьми, под руководством которых выполняется поставленная задача. Здесь возникает этика для роботов, использующих искусственный интеллект. Этика робототехники касается не только управления выполняемой работой, но и влияния роботов с искусственным интеллектом на окружающих их людей, находящихся в зоне выполнения задачи.

2.1. Ответственная робототехника

Ответственная робототехника (Memarian & Doleck, 2023) – это робототехника, целью которой является помощь человеку в выполнении различных задач: от повседневных домашних дел до сложных операций и даже полетов в космос для совершения научных открытий. Однако, являясь основной частью ИИ, робототехника не должна наносить вред человеку и окружающей его среде. Именно это должно стать целью создания ответственной робототехники, именно это должно лежать в основе создания интеллектуальной робототехники на базе ИИ. Следует отметить, что ответственная робототехника не может пойти по неверному пути, поскольку входные данные преобразуются в выходные. Для этого необходимо разработать этические протоколы.

Необходимо ответить на важный вопрос: зачем нам нужны роботы? Они нужны для того, чтобы помогать людям либо выполнять то, что люди делать не могут. Роботы работают на языках программирования, используя цифровые данные. Интеллектуальная робототехника должна понимать проблемы, прежде чем она сможет решать их.

В настоящее время на производстве применяются различные виды роботов, в том числе с искусственным интеллектом (Brooks, 1991). Их можно использовать в спасательных операциях на шахтах, для колонизации других планет или космических объектов. В целях безопасности робототехника должна быть отправлена в космическое пространство раньше самих людей. Пока не найдена другая планета, похожая на Землю, но человечество живет надеждой, и с надеждой люди достигли невероятного прогресса во всех отраслях. Можно попытаться создать такой ИИ и роботов, которые помогут сохранить жизнь и благополучие на Земле, и одновременно создать условия для жизни на других космических телах.

Роботы на основе ИИ могут помочь и при экстремальных лесных пожарах. Они могут извлекать из мусора металлы и другие ценные вещества, автоматически отделять одноразовый пластик от других видов мусора. Есть работа, не предназначенная для человека, и тогда на помощь приходят машины и роботы, основанные на искусственном интеллекте. Вместе с тем появляется и ответственность человека за то, чтобы сделать эти машины безопасными для использования. Еще раз подчеркнем, что ИИ находится на стадии зарождения и раннего развития, поэтому необходимо соблюдать этические нормы во всех случаях применения ИИ.

3. Решения в области этики искусственного интеллекта и робототехники

Если задана программа и известно, что машина всегда следует заложенным в нее правилам, то можно быть уверенным, что ответственная робототехника не может пойти по ложному пути. Существует две характеристики ИИ с точки зрения его использования и получаемых результатов. Они представлены следующим образом (Kumar et al., 2023):

1. Хороший ИИ.

Хороший ИИ – это полезный ИИ, разработанный для выполнения задач и проверяемый с помощью методов «черного ящика» и «белого ящика». Такой ИИ требует определенных входных данных и выдает предсказуемые результаты. Он может использовать обычные инструменты распознавания образов (Duda & Hart, 2006); к примеру, с помощью метода опорных векторов на основе дерева решений прогнозируется вероятность возникновения лейкемии. Эти алгоритмы не могут причинить никому вреда и обычно имеют заранее заданные выходные параметры. Другие области применения такого ИИ – оборона, полеты самолетов, запуск ракет, прогнозирование состояния здоровья, медицинские операции. Таким образом, эти алгоритмы можно назвать хорошим ИИ.

2. Плохой ИИ.

Алгоритм ИИ может нанести вред, используя необъективные данные, нарушая конфиденциальность, и по многим другим причинам. Проблемы могут вызвать различные приложения для обработки изображений, редактирования видео, создания поддельных профилей и фейковых новостей, взлома, кражи интеллектуальной собственности и т. д. Все это может причинить ущерб личной и профессиональной жизни людей.

Все основные проблемы, требующие решения, являются результатом использования плохого ИИ. Хороший ИИ отвечает требованиям этики и не наносит вреда. В нем, как правило, используются алгоритмы машинного обучения (Bishop, 2006; Palladino, 2023) для поиска решений и работы над проблемами. И все же для большей безопасности должны быть разработаны рекомендации для всех видов ИИ – хорошего и плохого, простого ИИ или AGI (general intelligence-based AI) – ИИ, основанного на общем интеллекте. Для любого из этих видов ИИ и робототехники с ИИ необходимо проводить проверки как по методу «черного ящика», так и по методу «белого ящика». Эти проверки позволяют в определенной степени предотвратить ошибочные результаты. Тестирование по методу «черного ящика» может выполнить любой человек, владеющий компьютерной грамотностью, в то время как тестирование по методу «белого ящика» – более комплексное, оно предполагает работу с кодом для выяснения причин возникшей ошибки. Таким образом, проблема решается в корне. Тестирование по методу «белого ящика» должно широко использоваться в отношении этического ИИ в робототехнике и интернете вещей.

3.1. Защита частной жизни

Такие инструменты на основе искусственного интеллекта, как «помощники по созданию текстов» и «умный ответ», могут вызывать опасения по поводу конфиденциальности (Zhang et al., 2021), поскольку создается впечатление, что ваши электронные письма читаются искусственным интеллектом и могут быть использованы не по назначению. Проблемы защиты частной жизни не ограничиваются электронной почтой. Они могут распространяться на конфиденциальность данных, когда существует риск утечки информации, и на личную конфиденциальность, когда под угрозой оказывается профиль пользователя аппаратного/программного обеспечения ИИ. Это могут быть данные о личности пользователя, о его компании, семье или имуществе. Кроме того, любое посягательство на частную жизнь является преступлением, поэтому инструменты и приложения на основе ИИ должны быть защищены от атак на неприкосновенность частной жизни или вирусных угроз. Приложения на основе искусственного интеллекта должны быть сделаны таким образом, чтобы избежать атак вирусов. Кроме того, сами приложения ИИ могут генерировать данные о просмотре веб-страниц и других действиях пользователя; обо всем этом следует позаботиться до начала использования инструмента ИИ.

Решением этой проблемы являются анализ собственных действий и установка соответствующих патчей на системы, использующие ИИ, то есть установка защиты от вредоносного ПО и вирусов. Для других приложений, использующих автоматическое наполнение на основе искусственного интеллекта, необходимо требовать от производителя соблюдения установленных норм для инструментов искусственного интеллекта. Только так можно обеспечить безопасность наших данных.

3.2. Право собственности

С развитием искусственного интеллекта возникает проблема прав собственности. Если изначально ИИ помогал художникам, авторам песен, сценаристам и создателям фильмов, то теперь он захватил все эти области. Кто научил ИИ всему этому? Ответ – мы сами. Программы на основе искусственного интеллекта были обучены

на сотнях и тысячах созданных людьми произведений искусства, фотографий, чатов и текстов. Когда ИИ генерирует, скажем, новое изображение, то он использует тысячи произведенных человеком предметов, а значит, заслуга искусственного интеллекта в создании новых изображений принадлежит и людям, которые не только создали исходное изображение, но и научили ИИ рисовать или, к примеру, петь.

Решение этой проблемы можно представить следующим образом. Существуют традиционные художники и художники на основе ИИ и цифровых искусств. Понятие искусства должно быть ограничено тем, что создано живописцами; аналогично следует рассуждать и в отношении других творцов, будь то сценаристы, музыканты и т. д.

3.2.1. Традиционное искусство

Традиционные художники придерживаются как освященных веками, так и новых подходов к созданию произведений искусства. Многие художники создают произведения в традиционных цветах и стилях, кто-то выбирает акриловые краски, а кто-то старое доброе масло. Другие работают со стеклом или глиной. Все это – примеры традиционных способов создания произведений искусства. Для них искусство – не только профессия, но и средство к существованию, страсть, источник любви и предмет поклонения. Большинство художников пишут не только для души, но и для получения побочного дохода, поэтому они могут пострадать не так сильно, как те, кто полностью полагается на творчество.

С развитием искусственного интеллекта, появлением новых потребностей и технологий старые способы создания произведений искусства могут исчезнуть. Новые технологии позволяют создавать произведения искусства быстрее, как правило, дешевле и с большей прибылью (Scimeca & Bonfiglio, 2023).

Однако большинство людей все же предпочитают традиционные произведения искусства. Привычные способы их создания требуют больше усилий, чем сравнимое по качеству цифровое искусство. Для многих освоение нового направления является непростой задачей, поэтому они придерживаются старых способов создания произведений искусства. Поначалу цифровое искусство также нелегко освоить, но когда художник овладеет им, то его развитие не потребует больших усилий.

3.2.2. Искусство с применением технологий и искусственного интеллекта

Художники, работающие в направлении техно и ИИ, используют те или иные технологии или искусственный интеллект для создания произведений искусства любого рода, будь то музыка, сценарии или картины. Они могут использовать такие инструменты, как программное обеспечение, 2D- или 3D-печать, искусственный интеллект и роботизированные руки. Изучив этот инструментарий, они могут погрузиться в безграничный мир творчества. Инструменты, управляемые искусственным интеллектом, еще более интересны, хотя для создания шедевров в музыке и живописи может потребоваться написать несколько строк кода. Здесь художник может работать как в сотрудничестве, так и самостоятельно, как создавать произведения с нуля, так и модифицировать и улучшать чужие работы.

Работы могут быть созданы на основе произведений, которые не принадлежат художнику, создающему новую работу. В таком случае юридически владелец оригинального произведения искусства обладает авторскими правами на него.

До сих пор не существует четкого законодательства, регулирующего эту сферу. В этом случае могут пострадать обе стороны: и цифровой художник, поскольку он вложил свои навыки работы с искусственным интеллектом в чужое произведение, и автор оригинального произведения, не получивший заслуженного вознаграждения. Пока правовые вопросы в этой сфере не решены, преимущество остается за автором оригинального произведения.

В данной ситуации как традиционные художники, так и те, кто работает с цифровыми технологиями и искусственным интеллектом испытывают огромное давление. Проблемы возникают в отношении авторских прав, лицензий на использование технологий, вопросов оплаты, репутации художника, прав собственности на произведения искусства, подтверждения их подлинности.

3.2.3. Решения

Искусственный интеллект и робототехника обучаются на тысячах созданных человеком произведений искусства, фотографий, сценариев и т. д. Эти обучающие данные используются для создания новых произведений искусства. Однако не всегда понятно, как найти создателей тех произведений искусства, на основе которых искусственный интеллект сгенерировал свое произведение. Иногда вклад заключается лишь в использовании одного оттенка цвета, а в другом случае используется целиком лицо, обработанное фильтром. Необходимо определить, что было взято из исходных обучающих данных, а что создано самим искусственным интеллектом. Юридически решение можно сформулировать следующим образом:

1. Если художественное произведение, созданное с помощью искусственного интеллекта, имеет более 80 % сходства с оригинальным произведением в обучающих данных, то создатель оригинального произведения и цифровой художник могут договориться о разделе прибыли или запрете на продажу нового произведения по желанию создателя оригинального произведения. Последний может купить работу, созданную цифровым художником, исходя из количества часов, потраченных им на редактирование исходного произведения.

2. В случае если доля оригинала составляет менее 80 % цифрового произведения, создатель оригинала может претендовать на часть прибыли от продажи работы и не может запретить цифровому художнику продавать ее.

3. Если создатель оригинального произведения пожелает работать вместе с цифровым художником, то они смогут разделить прибыль; такое сотрудничество может привести к новым высотам в создании невиданных ранее произведений искусства.

Такие решения могут гармонизировать рынок прав собственности на произведения искусства.

3.3. Пути к достижению ответственной робототехники

Среди проблем ответственной робототехники нужно выделить следующие (Stahl et al., 2023):

1. Конкурирующие роботы. По мере развития робототехники с искусственным интеллектом могут возникнуть такие проблемы, как противостояние роботов, созданных в различных странах. Эти контакты должны быть мирными; роботы не должны бороться друг с другом, они должны работать совместно, не создавая глобальной напряженности и конфликта интересов.

2. Полностью автономные роботы. Эти роботы, обладающие самосознанием, имеющие собственные мыслительные процессы и способные самостоятельно принимать решения, будут созданы на основе общего искусственного интеллекта (Artificial General Intelligence, AGI). Они находятся в стадии создания, и, насколько нам известно, ни один робот на базе AGI еще не используется. На таких роботов должны быть наложены особые ограничения.

3. Сбои в работе роботов на основе ИИ. Подобные проблемы могут представлять реальную угрозу для нормального функционирования того процесса, для которого был создан робот. Единственный способ решения этой проблемы – вывод робота из строя и установка программ, необходимых для устранения неполадок. После этого проводят соответствующее тестирование, а затем того же или нового робота вновь запускают в работу.

Решение заключается в создании универсальных машин, не конкурирующих между собой для достижения результатов и работающих в соответствии с этикой благополучия человека. Для этого необходимо на глобальном уровне договориться о нейтральности ИИ и робототехники, принятии и соблюдении законов их использования для достижения взаимовыгодных результатов. Таким образом, страны мира должны подписать юридические документы, гарантирующие сотрудничество как в области ИИ, так и в области робототехники. Договоренность должна предусматривать, что робототехнические устройства, создаваемые странами в оборонном, государственном, общественном и частном секторах, могут использоваться только с одобрения всего мирового сообщества.

3.3.1. Беспилотные автомобили на основе искусственного интеллекта

Беспилотный автомобиль с искусственным интеллектом должен не только доехать из точки А в точку Б, но и соблюдать правила дорожного движения, ездить по соответствующим дорогам, правильно парковаться, соблюдать скоростной режим, не наезжать на людей и животных по пути следования. Лишь при соблюдении этих условий беспилотный автомобиль может быть выпущен на дорогу. Недопустимы ситуации, подобные той, которая произошла несколько лет назад, когда беспилотный автомобиль столкнулся на дороге с другим автомобилем, определив это как ошибку. Согласно этике ИИ, такие автомобили не должны использоваться на дорогах, пока не будут пройдены все обязательные проверки на этику ИИ.

Следует отметить, что какого-либо одного закона в области робототехники будет недостаточно. Рассмотрим проблему этики беспилотных автомобилей на примере общей этики робототехники. Каждая область применения робототехники отличается от другой, поэтому сначала необходимо дать определения, затем указать, какую роль должны выполнять роботы на основе искусственного интеллекта. Затем юристы определяют, какие организации и субъекты могут быть затронуты процессами с участием робота на основе искусственного интеллекта; для каждого отдела разрабатывается схема безопасной работы. Отдел по этике совместно с техническим отделом по применению роботов должен разработать рекомендации по безопасному использованию роботов. Когда компания, создающая роботов, будет готова к их внедрению, отдел этических стандартов ИИ проводит проверку всего процесса. Лишь после получения одобрения всех сторон роботы могут быть допущены к работе (Leeson & Coyne, 2005).

3.3.2. Искусственный интеллект, робототехника и проблемы занятости

С появлением искусственного интеллекта происходит автоматизация существующих областей, что может привести к исчезновению некоторых рабочих мест. Возможными выходами из этой ситуации являются обучение и переобучение. Но такая возможность не гарантируется во всех областях, а также недоступна для некоторых людей по причине их возраста или инвалидности. В таких случаях работодатель должен тщательно подойти к вопросу увольнений. Это этические проблемы, которые приходится решать в качестве побочного эффекта от того, что ИИ выполняет человеческую работу (Duan, et al., 2019). У человека есть огромный потенциал, который он может раскрыть, существует множество новых областей, которые можно исследовать, имея государственное или частное финансирование. Однако переход из одной области в другую должен быть плавным, а компании должны помогать сотрудникам найти новую работу, соответствующую их способностям, заслугам, целям и размеру вознаграждения. Кроме того, должна быть предоставлена гарантия, скажем, на пять лет работы. Уязвимые категории населения должны сохранить свои рабочие места, их нельзя увольнять, как это происходит в 2023 году во всем мире.

Существует множество приложений, которые могут выполнять работы на основе искусственного интеллекта и робототехники. Это не означает, что необходимо провести сокращения рабочих мест и увольнения. Роботы не должны отнимать рабочие места, не создавая новых взамен. Как оборудование места для нового питомца в доме или установка новой люстры не отнимают у вас время для сна, так же должно обстоять дело и с искусственным интеллектом и робототехникой. Это единственный путь вперед – принять изменения, которые принесли с собой ИИ и робототехника, и ожидать появления новых рабочих мест. В то же время все нужно делать осторожно, учитывая ограничения, налагаемые этикой искусственного интеллекта (Hellwig et al., 2019).

3.3.3. Языковые модели на основе искусственного интеллекта

Искусственный интеллект находит широкое применение в больших языковых моделях (Large Language Models, LLM). В 2022 году наблюдался невиданный ранее рост LLM на основе искусственного интеллекта (Ferreira & Lipoff, 2023, Glaser, et al., 2019). То одна, то другая модель оказывались в центре внимания и били рекорды по производительности и точности решения задач, а некоторые по обоим параметрам сразу. При использовании LLM возникают такие проблемы, как непредсказуемость результатов, предвзятость, проблемы конфиденциальности, ошибки при передаче содержания, языковые ошибки и многие другие (Díaz-Rodríguez et al., 2023). Для дальнейшего развития LLM необходимо проводить оценку программного обеспечения искусственного интеллекта по методу «белого ящика», о чем говорилось в начале данного раздела. Проверка по этому методу позволяет предсказать следующий результат при заданной комбинации входных данных. Это должно свести к минимуму такие проблемы, как те, что возникли два года назад у одного из технологических гигантов в связи с использованием ошибочной рекомендательной системы, от которой пострадали многие группы людей.

Заключение

После установки и проверки программного обеспечения машина всегда следует правилам, заложенным в ее программу, и можно быть уверенным, что ответственная робототехника с искусственным интеллектом не пойдет по ложному пути. В данной

работе мы изучили ряд этических вопросов, распространенных в современном мире, и предложили новые решения этих проблем. Кроме того, было рассмотрено сочетание робототехники с искусственным интеллектом с точки зрения его потенциального использования и этики применения в будущем. Решения для многих других этических проблем еще предстоит разработать, что должно стать темой дальнейших исследований.

Список литературы

Agarwal, A., & Stoff, B. (2023). Ethics of using generative pretrained transformer and artificial intelligence systems for patient prior authorizations. *Journal of the American Academy of Dermatology*, *20*, 23–34. https://doi.org/10.1016/j.jaad.2023.04.030

Bishop, C. M. (2006). *Pattern recognition and machine learning*. New York: Springer. https://clck.ru/37AU6Z

Brooks, R. A. (1991). New approaches to robotics. *Science*, *253*(5025), 1227–1232.

Critchlow, A. J. (1985). *Introduction to robotics*. Macmillan Pub Co.

De Felice, F., Petrillo, A., De Luca, C., & Baffo, I. (2022). Artificial Intelligence or Augmented Intelligence? Impact on our lives, rights and ethics. *Procedia Computer Science*, *200*, 1846–1856. https://doi.org/10.1016/j.procs.2022.01.385

Hellwig, J., Huggett, S., & Siebert, M. (2019). *Artificial Intelligence: How knowledge is created, transferred, and used*. Elsevier. https://doi.org/10.17632/7ydfs62gd6.2

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges, and research agenda. *International Journal of Information Management*, *48*, 63–71. https://doi.org/10.1016/j.ijinfomgt.2019.01.021

Duda, R. O., & Hart, P. E. (2006). *Pattern classification*. John Wiley & Sons.

Ferreira, A. L., & Lipoff, J. B. (2023). The complex ethics of applying ChatGPT and language model artificial intelligence in dermatology. *Journal of the American Academy of Dermatology*, *89*(4), e157-e158. https://doi.org/10.1016/j.jaad.2023.05.054

Glaser, J. I., Benjamin, A. S., Farhoodi, R., & Kording, K. P. (2019). The roles of supervised machine learning in systems neuroscience. *Progress in Neurobiology*, *175*, 126–137. https://doi.org/10.1016/j.pneurobio.2019.01.008

Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, & Marcelo Sánchez Sorond. (2021). AI, Robotics, and Humanity: Opportunities, Risks, and Implications for Ethics and Policy. In J. von Braun et al. (Eds.), *Robotics, AI, and Humanity*. https://doi.org/10.1007/978-3-030-54173-6_1

Kumar, P., Chauhan, S., & Kumar, L. A. (2023). Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions. *Engineering Applications of Artificial Intelligence*, *120*, 105894. https://doi.org/10.1016/j.engappai.2023.105894

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y*, *1*, 511.

Lesandrini, J., Idris, M. Y., & Reis, D. S. (2023). The Ethics of Artificial Intelligence and Machine Learning. *Journal of Radiology Nursing*, *42*(3), 265–266. https://doi.org/10.1016/j.jradnu.2023.05.001

Memarian, D., & Doleck, T. (2023). Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review. *Computers and Education: Artificial Intelligence*, *5*, 100152, https://doi.org/10.1016/j.caeai.2023.100152

Mueller, V. C. (2012). Introduction: philosophy and theory of artificial intelligence. *Minds and Machines*, *22*(2), 67–69. https://doi.org/10.1007/s11023-012-9278-y

Palladino, N. (2023). A 'biased' emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*, *47*(5), 102479. https://doi.org/10.1016/j.telpol.2022.102479

Rich, E., Knight, K., & Nair, S. (2009). *Artificial Intelligence*. Tata McGraw Hill.

Saveliev, A. M., Zhurenkov, D. A., Poikin, A. E., & Berkutova, T. A. (2021). Ethics of Artificial Intelligence and Post-non-classical Scientific Rationality. *IFAC-PapersOnLine*, *54*(13), 397–401. https://doi.org/10.1016/j.ifacol.2021.10.480

Schank, R. C. (1991). Where's the AI? *AI magazine*, *12*(4), 38. https://doi.org/10.1609/aimag.v12i4.917

Scimeca, M., & Bonfiglio, R. (2023). Comment on redefining authorship in the era of artificial intelligence: balancing ethics, transparency, and progress. *ESMO Open*, *8*(5), 101635. https://doi.org/10.1016/j.esmoop.2023.101635

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26–33. https://doi.org/10.1109/msp.2018.2701164

Stahl, B. C., Brooks, L., Hatzakis, T., Santiago, N., & Wright, D. (2023). Exploring ethics and human rights in artificial intelligence – A Delphi study. *Technological Forecasting and Social Change*, *191*, 122502. https://doi.org/10.1016/j.techfore.2023.122502

Stahl, B. C. (2021). Perspectives on Artificial Intelligence. In *Artificial Intelligence for a Better Future. SpringerBriefs in Research and Innovation Governance* (pp. 7–17). Springer, Cham. https://doi.org/10.1007/978-3-030-69978-9_2

Turing, A. M. (2009). *Computing machinery and intelligence* (pp. 23–65). Springer Netherlands.

Xiao-Fan, L., Zhaoyang, W., Wei, Zh., Guoyu, L., & Gwo-Jen, H. (2023). Technological support to foster students' artificial intelligence ethics: An augmented reality-based contextualized dilemma discussion approach. *Computers & Education*, *201*, 104813. https://doi.org/10.1016/j.compedu.2023.104813

Zhang, Y., Wu, M., Yijun Tian, G., Zhang, G., & Lu, J. (2021). Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems*, *222*, 106994. https://doi.org/10.1016/j.knosys.2021.106994

Информация об авторе

Ядав Нидика – PhD, независимый исследователь
Адрес: 110074, Индия, г. Дели, Чаттапур Анклав Фейз II
E-mail: yadavnidhika68@gmail.com
ORCID ID: https://orcid.org/0000-0002-0165-6453
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195398958
WoS ID: https://www.webofscience.com/wos/author/record/2269009
Google Scholar ID: https://scholar.google.com/citations?user=fndffSwAAAAJ

Конфликт интересов

Автор сообщает 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: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 23 июля 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.41

Ethics of Artificial Intelligence and Robotics: Key Issues and Modern Ways to Solve Them

Nidhika Yadav

Independent Researcher
New Delhi, India

Keywords

artificial intelligence,
ChatGPT,
cyber security,
data privacy,
digital technologies,
ethics,
law,
robot,
robotics,
safety

Abstract

Objective: modern achievements in the development and dissemination of digital technologies have attracted the attention of scholars and practitioners to the discussion of key ethical issues related to artificial intelligence and robotics. Hence, this study presents the most relevant of these issues, posing new challenges for legal scholars and practitioners to develop the regulation of artificial intelligence and robotics in terms of technology moralization.

Methods: the research used practice- and risk-oriented approaches, complemented by multidisciplinary analysis of documents (European principles and codes of ethics) and studies, including those devoted to various problems of artificial intelligence and robotics.

Results: the article identifies key ethical issues in the field of artificial intelligence and robotics. It is established that the key ethical issues involved can be solved if they are legally formalized and implemented at the international level. The algorithm proposed by the author, based on the analysis of the digital technologies application, will allow improving the moral actions of technologies in the process of their decision making.

Scientific novelty: the article presents the latest ethical problems that concern scientists and practitioners in the field of artificial intelligence and robotics, and the methods of their solution by ethical and legal means aimed at moralizing technology and increasing its responsibility.

Practical significance: all solutions presented in the article have practical significance and are ready for wide implementation at the international level. Their formalization in normative form and subsequent compliance will reduce the harm that artificial intelligence may cause in applied fields, including robotics using artificial intelligence. Regulatory, including legislative, decisions must therefore be taken as soon as possible to ensure that artificial intelligence and robotics become reliable tools for these systems to be used at work, at home, and in other areas such as shopping centers, stores, schools, universities, etc.

For citation

Yadav, N. (2023). Ethics of artificial intelligence and robotics: key issues and modern ways to solve them. *Journal of Digital Technologies and Law, 1*(4), 955–972. https://doi.org/10.21202/jdtl.2023.41

References

Agarwal, A., & Stoff, B. (2023). Ethics of using generative pretrained transformer and artificial intelligence systems for patient prior authorizations. *Journal of the American Academy of Dermatology*, *20*, 23–34. https://doi.org/10.1016/j.jaad.2023.04.030

Bishop, C. M. (2006). *Pattern recognition and machine learning*. New York: Springer. https://clck.ru/37AU6Z

Brooks, R. A. (1991). New approaches to robotics. *Science*, *253*(5025), 1227–1232.

Critchlow, A. J. (1985). *Introduction to robotics*. Macmillan Pub Co.

De Felice, F., Petrillo, A., De Luca, C., & Baffo, I. (2022). Artificial Intelligence or Augmented Intelligence? Impact on our lives, rights and ethics. *Procedia Computer Science*, *200*, 1846–1856. https://doi.org/10.1016/j.procs.2022.01.385

Hellwig, J., Huggett, S., & Siebert, M. (2019). *Artificial Intelligence: How knowledge is created, transferred, and used*. Elsevier. https://doi.org/10.17632/7ydfs62gd6.2

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, 101896. https://doi.org/10.1016/j.inffus.2023.101896

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial intelligence for decision making in the era of Big Data – evolution, challenges, and research agenda. *International Journal of Information Management*, *48*, 63–71. https://doi.org/10.1016/j.ijinfomgt.2019.01.021

Duda, R. O., & Hart, P. E. (2006). *Pattern classification*. John Wiley & Sons.

Ferreira, A. L., & Lipoff, J. B. (2023). The complex ethics of applying ChatGPT and language model artificial intelligence in dermatology. *Journal of the American Academy of Dermatology*, *89*(4), e157-e158. https://doi.org/10.1016/j.jaad.2023.05.054

Glaser, J. I., Benjamin, A. S., Farhoodi, R., & Kording, K. P. (2019). The roles of supervised machine learning in systems neuroscience. *Progress in Neurobiology*, *175*, 126–137. https://doi.org/10.1016/j.pneurobio.2019.01.008

Joachim von Braun, Margaret S. Archer, Gregory M. Reichberg, & Marcelo Sánchez Sorond. (2021). AI, Robotics, and Humanity: Opportunities, Risks, and Implications for Ethics and Policy. In J. von Braun et al. (Eds.), *Robotics, AI, and Humanity*. https://doi.org/10.1007/978-3-030-54173-6_1

Kumar, P., Chauhan, S., & Kumar, L. A. (2023). Artificial Intelligence in Healthcare: Review, Ethics, Trust Challenges & Future Research Directions. *Engineering Applications of Artificial Intelligence*, *120*, 105894. https://doi.org/10.1016/j.engappai.2023.105894

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *JL Econ. & Pol'y*, *1*, 511.

Lesandrini, J., Idris, M. Y., & Reis, D. S. (2023). The Ethics of Artificial Intelligence and Machine Learning. *Journal of Radiology Nursing*, *42*(3), 265–266. https://doi.org/10.1016/j.jradnu.2023.05.001

Memarian, D., & Doleck, T. (2023). Fairness, Accountability, Transparency, and Ethics (FATE) in Artificial Intelligence (AI) and higher education: A systematic review. *Computers and Education: Artificial Intelligence*, *5*, 100152, https://doi.org/10.1016/j.caeai.2023.100152

Mueller, V. C. (2012). Introduction: philosophy and theory of artificial intelligence. *Minds and Machines*, *22*(2), 67–69. https://doi.org/10.1007/s11023-012-9278-y

Palladino, N. (2023). A 'biased' emerging governance regime for artificial intelligence? How AI ethics get skewed moving from principles to practices. *Telecommunications Policy*, *47*(5), 102479. https://doi.org/10.1016/j.telpol.2022.102479

Rich, E., Knight, K., & Nair, S. (2009). *Artificial Intelligence*. Tata McGraw Hill.

Saveliev, A. M., Zhurenkov, D. A., Poikin, A. E., & Berkutova, T. A. (2021). Ethics of Artificial Intelligence and Post-non-classical Scientific Rationality. *IFAC-PapersOnLine*, *54*(13), 397–401. https://doi.org/10.1016/j.ifacol.2021.10.480

Schank, R. C. (1991). Where's the AI? *AI magazine*, *12*(4), 38. https://doi.org/10.1609/aimag.v12i4.917

Scimeca, M., & Bonfiglio, R. (2023). Comment on redefining authorship in the era of artificial intelligence: balancing ethics, transparency, and progress. *ESMO Open*, *8*(5), 101635. https://doi.org/10.1016/j.esmoop.2023.101635

Stahl, B. C., & Wright, D. (2018). Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, *16*(3), 26–33. https://doi.org/10.1109/msp.2018.2701164

Stahl, B. C., Brooks, L., Hatzakis, T., Santiago, N., & Wright, D. (2023). Exploring ethics and human rights in artificial intelligence – A Delphi study. *Technological Forecasting and Social Change*, *191*, 122502. https://doi.org/10.1016/j.techfore.2023.122502

Stahl, B. C. (2021). Perspectives on Artificial Intelligence. In *Artificial Intelligence for a Better Future. SpringerBriefs in Research and Innovation Governance* (pp. 7–17). Springer, Cham. https://doi.org/10.1007/978-3-030-69978-9_2

Turing, A. M. (2009). *Computing machinery and intelligence* (pp. 23–65). Springer Netherlands.

Xiao-Fan, L., Zhaoyang, W., Wei, Zh., Guoyu, L., & Gwo-Jen, H. (2023). Technological support to foster students' artificial intelligence ethics: An augmented reality-based contextualized dilemma discussion approach. *Computers & Education*, *201*, 104813. https://doi.org/10.1016/j.compedu.2023.104813

Zhang, Y., Wu, M., Yijun Tian, G., Zhang, G., & Lu, J. (2021). Ethics and privacy of artificial intelligence: Understandings from bibliometrics. *Knowledge-Based Systems*, *222*, 106994. https://doi.org/10.1016/j.knosys.2021.106994

Author information

Yadav Nidhika – Ph.D., Independent Researcher
Address: Chattarpur Enclave Phase II Delhi-110074, India
E-mail: yadavnidhika68@gmail.com
ORCID ID: https://orcid.org/0000-0002-0165-6453
Scopus ID: https://www.scopus.com/authid/detail.uri?authorId=57195398958
WoS ID: https://www.webofscience.com/wos/author/record/2269009
Google Scholar ID: https://scholar.google.com/citations?user=fndffSwAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 23, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:346.1:006.44:004.8
EDN: https://elibrary.ru/oppobg
DOI: https://doi.org/10.21202/jdtl.2023.42

Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы

Анна Константиновна Жарова

Институт государства и права Российской академии наук
г. Москва, Российская Федерация

Ключевые слова

GDPR,
алгоритмическая прозрачность,
защита данных,
информационная безопасность,
информационные технологии,
искусственный интеллект,
конфиденциальность,
персональные данные,
право,
цифровые технологии

Аннотация

Цель: сравнение современных подходов в праве к использованию в процессе принятия решений программных кодов и алгоритмов, отвечающих принципам прозрачности и открытости, а также возрастающим требованиям к обеспечению безопасности персональных и иных больших данных, полученных и обработанных алгоритмическим путем.

Методы: основными методами исследования принципа прозрачности алгоритмизированного принятия решений являлись формально-юридический и сравнительный анализ правовых актов и международных стандартов информационной безопасности, содержащихся в них принципов и правовых конструкций.

Результаты: определено, что развитие области стандартизации информационной безопасности, включение в правовые акты требований о разработке информационных технологий, соответствующих принципам прозрачности и открытости применяемых алгоритмов, позволит минимизировать риски, связанные с неправомерными обработкой больших пользовательских данных и получением информации об их частной жизни; выявлены связанные с реализацией алгоритмической прозрачности предложения в области правового регулирования обработки данных; сформулированы рекомендации, с опорой на которые законодатель может решать задачу обеспечения открытости логики работы алгоритмов информационных технологий с учетом современных стандартов информационной безопасности.

Научная новизна: состоит в обосновании новых тенденций и формируемых в соответствии с ними правовых подходов, позволяющих раскрыть логику обработки данных цифровыми и информационными технологиями, на основе характеристики общеевропейских стандартов концепции конфиденциальности при проектировании новых цифровых и информационных технологий принятия решений и защиты данных, новых правовых требований, предъявляемых к системам искусственного интеллекта, включая требование об обеспечении алгоритмической прозрачности, критериев обработки персональных данных, а также больших пользовательских данных. При этом защита данных рассматривается как система правовых, технических и организационных принципов, направленная на обеспечение конфиденциальности персональных данных.

Практическая значимость: обусловлена необходимостью изучения передового отечественного и международного опыта защиты частной жизни пользователей цифровых и информационных технологий, а также законодательного обеспечения требований об использовании алгоритмов, отвечающих принципам прозрачности и открытости обработки персональных данных с учетом необходимости обеспечения конфиденциальности на всех этапах жизненного цикла их обработки, что позволит обеспечить непрерывность управления безопасностью.

Для цитирования

Жарова, А. К. (2023). Достижение алгоритмической прозрачности и управление рисками информационной безопасности при принятии решений без вмешательства человека: правовые подходы. *Journal of Digital Technologies and Law*, *1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

Содержание

Введение

Все сложнее становятся модели информационных технологий, и все больше данных, связанных с человеком, они обрабатывают. Так, технологии интернета вещей собирают большой объем данных, в котором могут содержаться различные данные, включая большие пользовательские данные. У пользователя информационными технологиями (далее – ИТ) вызывает обеспокоенность невозможность контроля над действиями, осуществляемыми информационными технологиями, а также отсутствие понимания логики работы алгоритмов, обрабатывающих его данные, какие именно данные обрабатываются и каков конечный результат анализа данных. Желание понять критерии анализа обрабатываемых данных, а также необходимость обеспечения контроля за их перечнем привели законодателя к мысли о необходимости включения в правовые акты требования об использовании алгоритмов, отвечающих принципам прозрачности и открытости. Иными словами, необходимо раскрыть логику обработки данных информационными технологиями.

В такой научной области, как информатика, для описания прозрачности процессов, происходящих при функционировании информационных технологий, применяется термин «алгоритмическая прозрачность». В связи с необходимостью обеспечения защиты пользовательских данных этот термин был заимствован юридической наукой.

Термин «алгоритмическая прозрачность» в законодательстве Российской Федерации используется для описания регулирования отношений при применении систем искусственного интеллекта (далее – ИИ)[1]. Хотя ученые считают, что термин «алгоритмическая прозрачность» может применяться для описания более широкого круга отношений, выходящих за пределы функционирования ИИ (Кутейников и др., 2020; Гулемин, 2022).

В связи с такой многозначностью в первую очередь необходимо изучить понятие «алгоритмическая прозрачность», а далее на основании полученного исследования разобраться в предложениях, связанных с реализацией алгоритмической прозрачности в области правового регулирования обработки данных.

1. Понятие алгоритмической прозрачности

В Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 г.[2] проблема алгоритмической прозрачности систем искусственного интеллекта отнесена к концептуальным проблемным направлениям регулирования отношений в сфере технологий искусственного интеллекта и робототехники[3].

«Алгоритмическая прозрачность» информационной модели позволяет получить представление о логике функционирования информационной модели, реализуемой

---

1 Указ Президента Российской Федерации № 490 от 10.11.2019 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года). (2019). Собрание законодательства Российской Федерации, 41, ст. 5700.

2 Распоряжение Правительства Российской Федерации № 2129-р от 19.08.2020. (2020). Собрание законодательства Российской Федерации, 35, ст. 5593.

3 Там же.

ИИ при заданных входных данных. Однако необходимо сразу оговориться, что сложность алгоритмов ИИ не позволяет описать любой алгоритм ИИ так, чтобы его логика стала понятна обывателю. Наиболее простой с точки зрения восприятия происходящих алгоритмических этапов является линейная модель ИИ и ее математическая интерпретация. Наиболее сложной для понимания логики функционирования модели ИИ является глубокая архитектура ИИ[4].

Иными словами, алгоритмическая прозрачность – это объяснимость работы «ИИ и процесса достижения им результатов, недискриминационный доступ пользователей продуктов, которые созданы с использованием технологий искусственного интеллекта, к информации о применяемых в этих продуктах алгоритмах работы искусственного интеллекта»[5]. С точки зрения некоторых исследователей, технологические разработки в области ИИ и алгоритмов стали неотъемлемой частью государственного управления (Feijóo et al., 2020; Carlsson & Rönnblom, 2022; Balasubramaniam et al., 2023; Green, 2022).

2. Защитит ли пользовательские данные понимание логики работы алгоритма обработки данных?

В 1999 г. Л. Лессиг был одним из первых авторов, который отдавая должное правовым и социальным нормам в обеспечении правового регулирования отношений, возникающих в ИКТ-сфере, признал программный код равнозначной составляющей в области регулирования информационных отношений, именно он определяет архитектуру пространства ИКТ-сферы. Программный код позволяет достичь наилучшего результата в регулировании отношений, возникающих в информационной сфере (Lessig, 1999).

Программный код формализует логику работы алгоритма. Все чаще звучат предложения об обеспечении алгоритмической прозрачности программного обеспечения. «Прозрачность алгоритмов становится своеобразной формой контроля, а прозрачность алгоритмического принятия решений служит тому, чтобы несправедливые дискриминации могли быть обнаружены и оспорены» (Талапина, 2020). Хотя есть противоположная точка зрения. Так, некоторые ученые считают, что требование об алгоритмической прозрачности – это действия, направленные на взаимодействие разработчиков ИТ с органами власти в целях нормализации поведения граждан (Wang, 2022).

По нашему мнению, требование о прозрачности алгоритмов не принесет желаемого результата, поскольку разобраться в логике алгоритма ИИ не всегда под силу даже специалисту. В связи с этим несправедливые дискриминации, заложенные в алгоритмы ИИ, не всегда могут быть обнаружены и оспорены.

Анализируя тенденцию реализации алгоритмической прозрачности, попытаемся привести позиции за и против раскрытия логики алгоритма.

---

4 Корешкова, Т. (2020, 29 декабря). Объяснимый искусственный интеллект. Научно-технический центр ФГУП «ГРЧЦ». https://clck.ru/36h6w6

5 Указ Президента РФ № 490 от 10.11.2019 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 года). (2019). Собрание законодательства Российской Федерации, 41, ст. 5700.

Так, обыватель, возлагая надежду на раскрытие логики алгоритма, считает, что это позволит ему понять его логику, однако такие предложения, хотя и не безосновательны, но имеют свои недостатки. Во-первых, большинству людей, не имеющих компетенций в области программирования и разработки информационных технологий, раскрытие логики работы алгоритма не даст никакой информации. Во-вторых, если пользователь алгоритма, например, ИИ, разберется в его логике, то внесение изменений в алгоритм будет невозможно в связи с тем, что для этого потребуется пересмотреть весь заложенный в алгоритм математический инструментарий. В-третьих, раскрытие логики работы алгоритма не должно противоречить требованиям законодательства об интеллектуальной собственности, поскольку интеллектуальные права на алгоритмы принадлежат его правообладателям, разработчикам. Соответственно, раскрытие логики работы алгоритма может происходить в строго ограниченных случаях.

Существуют и иные позиции ученых, которые предлагают заменить раскрытие логики работы алгоритмов страхованием рисков, связанных с обеспечением информационной безопасности. Например, пользователь, садясь в самолет и доверяя свою жизнь перевозчику, предварительно не изучает логику работы программного обеспечения самолета. Все риски берут на себя перевозчик, страховщик и другие лица, ответственные за перевозку пассажиров (Остроумов, 2015). Разве в случае обработки данных мы не можем использовать эту же правовую схему регулирования отношений?

«Перевозчиками» пользовательских данных являются различные информационные посредники, например, провайдеры, операторы обработки персональных данных. Учитывая существующую высокую вероятность того, что раскрытие логики работы алгоритма фактически ничего не даст пользователю, то не будет ли более эффективным применение системы страхования к отношениям в ИКТ-сфере, как в случае с воздушными перевозками? В этом случае будут застрахованы риски «гибели» пользовательских данных или несанкционированного доступа к ним, а также ответственность информационных посредников или операторов персональных данных.

Однако и в этом случае есть свои подводные камни. Так, в случае с воздушными перевозками все этапы, начиная от создания самолета до его полета, жестко регламентируются нормами правового и технического регулирования, чего не происходит в случае создания алгоритмов, информационных моделей и их использования. Стандартизация информационных технологий в целях обеспечения информационной безопасности является добровольной. Обязательной стандартизации подлежат такие информационные системы, как критическая информационная инфраструктура Российской Федерации и системы, обрабатывающие персональные данные.

В связи с этим проведение аналогии между обеспечением безопасности пользователя ИТ через обеспечение алгоритмической прозрачности и безопасностью воздушных перевозок возможно только в условиях жесткой регламентации создания ИТ и их использования нормами правового и технического регулирования.

Вопрос доверия в области информационной безопасности волнует умы ученых разных государств (Cui et al., 2022; Bujold et al., 2022; Zhu et al., 2023). Доверие определяется как культурная ценность, которая иногда может вступать в противоречие с национальной политикой в области ИИ (Robinson, 2020; Xu et al., 2022; Li, 2022).

3. Сравнительный анализ принципов алгоритмической прозрачности

Эксперты Сообщества справедливости, подотчетности и прозрачности в области машинного обучения (Fairness, Accountability, and Transparency in Machine Learning – FAT) определяют пять принципов алгоритмической прозрачности: справедливость, проверяемость, объяснимость, ответственность разработчиков и точность работы[6]. Как видим, в предложениях Сообщества справедливости, подотчетности и прозрачности в области машинного обучения объяснимость логики работы ИИ стоит на третьем месте. Скорее всего, это связано именно с тем, что алгоритмическая открытость не во всех случаях может решить вопросы обеспечения безопасности пользователя ИТ.

Учеными предлагается дополнить эти пять принципов принципом внесения изменений в логику работы алгоритма ИИ в случае несогласия с ее функционированием (Малышкин, 2019; Gordon et al., 2022). Однако такие предложения вызывают у нас опасения, поскольку в этом случае возможно нарушение законодательства об интеллектуальной собственности. Большинство компаний не стремятся раскрывать свои алгоритмы и делать их прозрачными, «ссылаясь на потенциальные игры пользователей, которые могут негативно повлиять на предсказательную способность алгоритма» (Qiaochu et al., 2020; Stahl et al., 2022).

Со своей стороны хотели бы подчеркнуть, что отсутствие в сформулированных пяти принципах «возможности изменения логики работы ИИ» объяснимо. Такие алгоритмы разрабатываются коллективом программистов, изменение логики работы одной части алгоритма ИИ сделает неработоспособной математическую модель всего алгоритма (Varsha, 2023; Lang & Shan, 2000; Akter et al., 2022). Если бы человеческий мозг мог решить задачу обработки больших, неструктурированных данных, то алгоритмы ИИ были бы бесполезны.

В Российской Федерации в соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 г. принципами развития и использования ИИ, соблюдение которых обязательно, являются: защита прав и свобод человека, технологический суверенитет, целостность инновационного цикла, разумная бережливость, поддержка конкуренции, безопасность и прозрачность[7].

Под безопасностью понимается «недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий искусственного интеллекта»[8]. Прозрачность определена как «объяснимость работы искусственного интеллекта и процесса достижения им результатов, недискриминационный доступ пользователей продуктов, которые созданы с использованием технологий искусственного интеллекта, к информации о применяемых в этих продуктах алгоритмах работы искусственного интеллекта» (п. 19)[9].

---

6 Principles for Accountable Algorithms and a Social Impact Statement for Algorithms. https://clck.ru/36h7GL

7 Указ Президента РФ № 490 от 10.11.2019 (вместе с Национальной стратегией развития искусственного интеллекта на период до 2030 г.). (2019). Собрание законодательства Российской Федерации, 41, ст. 5700.

8 Там же.

9 Там же.

Подчеркнем, что, если Сообществом справедливости, подотчетности и прозрачности в области машинного обучения алгоритмическая прозрачность определена через пять принципов, то российское законодательство алгоритмическую прозрачность включило в принципы развития и использования ИИ. Принцип недискриминационного доступа пользователей ИИ к информации о применяемых алгоритмах работы ИИ пересекается с принципами, сформулированными Сообществом справедливости, подотчетности и прозрачности в области машинного обучения.

Не содержит законодательство Российской Федерации также требования об опубликовании правил, определяющих основные алгоритмические обработки пользовательских данных, в отличие от французского законодательства. Так, в соответствии с Законом Франции «О цифровой республике» от 7 октября 2016 г. такие правила должны публиковаться на сайте государственного органа (Талапина, 2020).

В Евросоюзе безопасность персональных данных резидентов Евросоюза (Su et al., 2023), а также прозрачность их обработки алгоритмами (Matheus et al., 2021; Kempeneer, 2021), в том числе ИИ (Kempeneer et al., 2023; de Bruijn et al., 2022), регулируются Регламентом защиты персональных данных (Stöger et al., 2021) – General Data Protection Regulation (далее – GDPR), вступившим в силу в 2018 г. (Mourby et al., 2021).

4. Разработка и принятие Общего регламента по защите данных

Несмотря на то, что защита частной жизни напрямую не связана с защитой персональных данных, их использование позволяет идентифицировать личность человека и соответственно получить информацию о его частной жизни. Таким образом, надежно защищенные персональные данные уменьшают риски получения информации о частной жизни лица (Bolton et al., 2021; Leerssen, 2023). Необходимость борьбы с различными нарушениями законодательства в области персональных данных и частной жизни лица, а также минимизация последствий таких деяний, способствовали разработке и принятию GDPR (Willems et al., 2022; Custers & Heijne, 2022).

Одним из первых дел, связанных с незаконным получением информации о частной жизни лица путем незаконного доступа к базе персональных данных, было дело Uber. Взломы базы персональных данных Uber произошли в 2014 и 2016 гг., что позволило злоумышленникам отслеживать местонахождение каждого пользователя Uber в режиме реального времени. В 2017 г. Федеральная торговая комиссия (далее – ФТС) обвинила Uber в отсутствии должного контроля доступа сотрудников к базам данных пользователей и водителей системы Uber, а также в нарушении системы обеспечения безопасности информации. В дальнейшем между Uber и ФТС было подписано соглашение, в рамках которого Uber обязалась проводить сторонние проверки в течение двадцати лет и реализовать программу защиты конфиденциальности[10].

В 2017 г. ФТС включила в соглашение дополнительные положения, обязывающие Uber проводить аудит их системы и представлять отчеты в ФТС, а также раскрывать информацию о вознаграждениях и условиях соглашений, которые Uber заключает с третьими лицами, осуществляющими мониторинг уязвимостей программного обеспечения Uber. В соответствии с последней редакцией соглашения Uber:

[10] Uber criminal complaint raises the stakes for breach response. https://clck.ru/37AXba

– может быть привлечена к гражданско-правовым санкциям, если она не уведомит ФТС об инцидентах, связанных с несанкционированным доступом к информации о пользователях и водителях Uber;

– запрещено искажать информацию об уровне защиты информации в системе, об условиях обеспечения конфиденциальности, безопасности и целостности личной информации, а также о том, как она контролирует внутренний доступ к личной информации потребителей;

– должна внедрить комплексную программу конфиденциальности и в течение 20 лет получать раз в два года независимые оценки обеспечения безопасности своей информационной системы, проводимые третьими лицами. Компания Uber должна предоставлять эти оценки в ФТС и подтверждать выполнение принятой программы конфиденциальности, которая должна содержать условия обеспечения безопасности, имеющиеся в соглашении с ФТС;

– обязана хранить информацию о местоположении пользователя в системе, защищенную паролем и шифром;

– обязана проводить ежегодное обучение сотрудников, ответственных за обработку личной информации, методам защиты данных и обеспечения безопасности, принятой в Uber, а также использовать новейшие методы контроля безопасности;

– обязана использовать передовые методы защиты данных для защиты персональных данных водителей;

– должна назначить одного или нескольких сотрудников для координации и контроля программы обеспечения безопасности и конфиденциальности, а также проводить регулярные оценки эффективности внутреннего контроля и процедур Uber, связанных с защитой личной информации и информации о географическом местоположении своих сотрудников и клиентов Uber;

– обязана использовать многофакторную аутентификацию, прежде чем любой сотрудник сможет получить доступ к конфиденциальной личной информации клиента, а также другие надежные методы обеспечения безопасности данных[11].

В связи с нарушениями, произошедшими в 2014 и 2016 гг., компания Uber заплатила штраф в размере 148 млн долларов[12]. 20 августа 2020 г. в отношении бывшего начальника службы безопасности Uber было возбуждено уголовное дело, в котором было предъявлено обвинение в воспрепятствовании правосудию и предполагаемой попытки сокрытия утечки данных, произошедшей в 2016 г.

5. Реализация общего регламента по защите данных

GDPR определяет право каждого на защиту своих персональных данных в соответствии с ч. 1 ст. 16 Договора о функционировании Европейского союза (TFEU)[13] и ч. 1

[11] Там же.

[12] Uber to Pay $148 Million Fine for Massive Data Breach That Exposed 57 Million Users' Personal Info. https://clck.ru/36h7RG

[13] Договор о функционировании Европейского союза [рус., англ.] (вместе со «Списком, предусмотренным в статье 38...», «Заморскими странами и территориями, к которым применяются положения части четвертой Договора...») (подписан в г. Риме 25.03.1957) (с изм. и доп. от 13.12.2007). СПС «КонсультантПлюс».

ст. 8 Хартии Европейского союза об основных правах[14] (далее – Хартия)[15], а также «право на неприкосновенность частной жизни» (ст. 7 Хартии)[16].

GDPR требует от компаний, обрабатывающих персональные данные резидентов Евросоюза или осуществляющих свою деятельность на территории государства Евросоюза, соблюдения не только правовых требований, но и организационно-технических, которые должны быть учтены разработчиками еще на этапе проектирования информационных технологий, и названных как «конфиденциальность при проектировании» (ст. 3 GDPR). Требования об обеспечении конфиденциальности в цифровом мире посредством «защиты персональных данных при проектировании и по умолчанию» утверждены European Data Protection Board (EDPB) в Руководстве 4/2019 «Встроенная защита данных и по умолчанию» (Guidelines 4/2019 on Article 25 Data Protection by Design and by Default)[17].

Реализация данных требований вызвала у компаний множество вопросов о процедурах их реализации. В связи с чем Европейский совет по защите данных – EDPB – и Европейский надзорный орган по защите данных (European Data Protection Supervisor – EDPS) представили разъяснения. В Заявлении EDPB 03/2021 «Положение о конфиденциальности», принятом Советом по защите частной жизни и конфиденциальности при использовании услуг электронной связи, указывается, что предлагаемое Положение ни при каких обстоятельствах не должно снижать уровень защиты, определенный в действующей Директиве 2002/58/EC[18]. Положение должно дополнять GDPR, предоставляя дополнительные надежные гарантии конфиденциальности и защиту всех типов электронных сообщений[19]. Директива 2002/58/EC охватывает обработку персональных данных и защиту конфиденциальности, включая требования об обеспечении безопасности сетей и услуг; конфиденциальности общения; доступа к сохраненным данным; обработке данных о трафике и местоположении; идентификации; общедоступных справочниках подписчиков, а также запрете коммерческих сообщений (спама)[20]. EDPB особое внимание уделяет безопасности персональных данных, обрабатываемых работодателями. EDPB четко определяет случаи и условия, при которых работодатели могут получить доступ к персональным данным сотрудников, а также ответственность за чрезмерный сбор данных с помощью технологий анализа и обработки данных. Например, применение работодателем систем геолокации, технологий постоянного контроля перемещений и поведения сотрудника.

---

14 Хартия Европейского союза об основных правах (2007/C 303/01) [рус., англ.] (Вместе с «Разъяснениями...» (2007/C 303/02)) (Принята в г. Страсбурге 12.12.2007). СПС «КонсультантПлюс».

15 Там же.

16 Charter of Fundamental Rights of the European Union. https://clck.ru/36h7Tn

17 Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020. https://clck.ru/36h7Ug

18 E-privacy Directive 2009/136/EC. https://clck.ru/36h7VG

19 Statement 03/2021 on the ePrivacy Regulation Adopted on 9 March 2021. https://clck.ru/36h7WF

20 E-privacy Directive 2009/136/EC. https://clck.ru/36h7VG

Поскольку функции EDPB и EDPS пересекаются, то для разграничения их деятельности был принят Меморандум о взаимопонимании между EDPB и EDPS[21], в соответствии с которым EDPB обеспечивает единство правоприменительной практики GDPR, а EDPS обеспечивает единство подходов национальных надзорных органов. При этом EDPB и EDPS могут издавать совместные документы по вопросам защиты персональных данных.

6. Концепция конфиденциальности при проектировании информационных технологий

Концепция конфиденциальности при проектировании была разработана задолго до принятия GDPR. Так, в 1995 г. в Директиву 95/46 / ЕС «О защите данных»[22] было включено положение о том, что «в целях защиты безопасности данных технические и организационные меры должны быть определены и приняты еще на стадии планирования системы обработки данных» (ст. 46 Директивы 95/46 / ЕС).

22 июня 2011 г. EDPS вынес на обсуждение концепцию изменения подхода к регулированию защиты персональных данных и обеспечению их конфиденциальности[23] в форме публичного мнения этой организации. В целях необходимости и целесообразности учета требований защиты персональных данных посредством конфиденциальности при проектировании ученые предложили изменить концепцию защиты персональных данных, изложив ее в следующих семи принципах[24]:

1. Меры обеспечения конфиденциальности при проектировании должны быть превентивными и учитывать возможные риски и угрозы, а не являться ответной реакцией на нарушения конфиденциальности.

2. Решение проблемы обеспечения конфиденциальности в информационных системах должно быть реализовано в системе еще на уровне ее разработки, а не являться опцией для пользователя.

3. Возможные риски и угрозы должны учитываться еще на этапе проектирования технологии, а также быть прописаны в стандартах информационной безопасности и учитывать контекст данных. Методы обеспечения безопасности персональных данных должны постоянно обновляться.

4. Конфиденциальность должна быть реализована на всех этапах жизненного цикла обработки персональных данных, это позволит обеспечить непрерывность управления безопасностью. Применяемые стандарты безопасности должны гарантировать конфиденциальность, целостность и доступность личных данных на протяжении всего их жизненного цикла, а также реализацию методов безопасного уничтожения, шифрования, контроля доступа и ведения журналов.

5. Должны обеспечиваться мониторинг, оценка и проверка соблюдения политик и процедур конфиденциальности, открытость и прозрачность в целях соблюдения

---

21 Memorandum of Understanding. https://clck.ru/36h7ic

22 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/36h7jM

23 The History of the General Data Protection Regulation. https://clck.ru/36h7jw

24 The Seven Principles. https://goo.su/mn8ob7

принципа подотчетности и создания условий для обеспечения доверия со стороны субъектов персональных данных и контрагентов, а также унификации деловой практики. Физическим лицам должны быть доступны информация о политиках и методах управления личной информацией, механизмы соблюдения требований и рассмотрения жалоб.

6. Не должен стоять выбор между безопасностью и функциональностью.

7. Права и интересы субъектов персональных данных должны быть основой для проектирования конфиденциальности.

Данные принципы были одними из первых, которые учли фактически все возможные риски нарушения обработки персональных данных. Однако предлагались и другие концепции[25].

7. Понятия «персональные данные» и «конфиденциальность» в соответствии с законодательством Европейского союза

В соответствии с GDPR под персональными данными понимается любая информация, относящаяся к физическому лицу, которое можно идентифицировать. В соответствии со ст. 4 GDPR к таким данным можно, например, отнести ссылку на идентификатор, такой как имя, идентификационный номер, данные о местоположении, онлайн-идентификатор, любые факторы, специфичные для физических, физиологических, генетических, ментальных, экономических, культурных или социальных идентичностей этого физического лица.

В тексте GDPR определение понятия «конфиденциальность» отсутствует, однако дается отсылка к Директиве 2002/58/EC Европейского парламента и Совета от 12 июля 2002 г. относительно обработки персональных данных и защиты конфиденциальности в секторе электронных коммуникаций (далее – Директива 2002/58/EC)[26]. GDPR использует понятие «персональные данные». По мнению EDPB[27], EDPS[28], а также ENISA[29] в контексте проектируемой конфиденциальности понятия «персональные данные» и «конфиденциальность» следует рассматривать как синонимы. Кроме того, руководящие рекомендации EDPB, EDPS, ENISA определяют, что для ситуаций, не имеющих особого значения, не должно делаться различий между защитой персональных данных и обеспечением конфиденциальности при проектировании и по умолчанию.

---

25 Langheinrich, M. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems: Distributed Systems Group Institute of Information Systems, IFW Swiss Federal Institute of Technology, ETH Zurich 8092 Zurich, Switzerland. https://clck.ru/36h7qq

26 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

27 EDPB – это независимый орган Европейского союза, созданный и функционирующий на основании GDPR. EDPB способствует обеспечению согласованного применения GDPR, для чего обладает рядом полномочий, установленных ст. 70 GDPR. В частности, в полномочиях этого органа находится издание руководства, рекомендаций и лучших практик применения GDPR.

28 EDPS – это независимый орган ЕС, контролирующий деятельность национальных надзорных органов, которые должны быть созданы в соответствии с разделом V GDPR.

29 Агентство Европейского союза по кибербезопасности ENISA. https://clck.ru/N598K

Однако такая общность в понимании защиты персональных данных и обеспечения конфиденциальности при проектировании и по умолчанию принимается не для всех случаев. В опубликованном мнении EDPS[30] «О защите конфиденциальности при проектировании и по умолчанию» (opinion on privacy by design and by default) делается различие между двумя понятиями – «конфиденциальность при проектировании» и «защита данных при проектировании» (privacy by design и data protection by design). Понятие «конфиденциальность при проектировании» используется для обозначения системы технологических мер, направленных на обеспечение конфиденциальности, выработанной в ходе международных дебатов за последние несколько десятилетий. Данное понятие определяет правовой режим информации, заключающийся в ограничении доступа к ней, и означает «защиту данных с помощью технологического проектирования»[31] (Zharova, 2020).

Под «защитой данных при проектировании» понимается предварительное решение вопросов защиты данных и конфиденциальности на этапе проектирования технологии для всех действий пользователя[32] (Zharova, 2019).

Обсуждения степени различия данных терминов продолжаются и до настоящего времени. Так, разработчики разъяснений о применении GDPR[33] пишут, что все еще существует неопределенность в отношении того, что означает конфиденциальность при проектировании и как ее можно реализовать. Такая проблема возникает в связи с тем, что, с одной стороны, Директива 95/46/EC (Directive 95/46/EC)[34] в некоторых государствах-членах реализуется не в полной мере. С другой – принцип конфиденциальности при проектировании, содержащийся в GDPR, определяет, что руководящие принципы безопасности данных требуют, чтобы организационные и технические меры были приняты еще на уровне планирования информационной системы. Например, принцип GDPR обеспечения целостности и конфиденциальности определяет необходимость защиты данных от несанкционированного доступа или их незаконной обработки, а также от случайной потери, уничтожения или повреждения[35]. Однако законодательство Евросоюза оставляет полностью открытым вопрос о принимаемых ответственными лицами защитных мерах. Например, достаточно ли анонимизации имени человека для реализации требований законодательства?

GDPR предлагает использовать шифрование или анонимизацию данных в качестве возможной меры обеспечения конфиденциальности при проектировании. Однако это предложение не позволяет понять, как эта мера в дальнейшем будет

30 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. https://clck.ru/36h7v3

31 GDPR Privacy by Design. https://clck.ru/36h7vZ

32 Data protection by design and default. https://goo.su/Hxoh2d

33 GDPR Privacy by Design. https://clck.ru/36h7vZ

34 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. https://clck.ru/36h7jM

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) of 27 April 2016. https://clck.ru/34U2FN

согласовываться с требованием GDPR об аутентификации пользователя и технической реализацией права на возражение.

В итоге авторы разъяснений о применении GDPR определили термин «конфиденциальность при проектировании» как «защиту данных с помощью технологического проектирования», они считают, что «в процедурах обработки данных лучше всего придерживаться защиты данных, когда она уже интегрирована в технологию на этапе ее проектирования»[36].

Заключение

Проблема защиты персональных данных, контроль принципов обработки больших пользовательских данных, защита частной жизни лица с каждым годом только обостряются. Необходимость обеспечения защиты персональных данных и частной жизни лица как пользователя ИТ ставит перед законодателем задачу обеспечения открытости логики работы алгоритмов информационных технологий. Например, для достижения этой цели в GDPR определено требование о реализации проектируемой конфиденциальности при разработке ИТ, которое было предложено еще в 1995 г. Требование о реализации принципа алгоритмической прозрачности в системах ИИ было предложено намного позже, в 2019 г., российскими законодателями, а зарубежными законодателями – в 2018 г.

Алгоритмы обработки данных только усложняются, в связи с чем все чаще звучат законодательные предложения о раскрытии логики их работы, например в системах ИИ; нужно понимать, что такие предложения можно реализовать не для всех алгоритмов. Объяснить сложный математический инструментарий простыми словами, которые будут понятны каждому обывателю, вряд ли удастся.

Однако это не значит, что не существует выхода из этой сложной технико-правовой ситуации. Мы считаем, что развитие области стандартизации информационной безопасности, включение в правовые акты требования о разработке ИТ, соответствующих требованиям стандартизации, позволит минимизировать риски, связанные с неправомерной обработкой больших пользовательских данных и получением информации о частной жизни лица.

Список литературы

Гулемин, А. Н. (2022). Пределы обработки больших объемов данных для целей получения информации о человеке: правовой аспект. *Электронное приложение к Российскому юридическому журналу*, *6*, 52–57. http://doi.org/10.34076/22196838_2022_6_52

Кутейников, Д. Л., Ижаев, О. А., Зенин, С. С., Лебедев, В. А. (2020). Алгоритмическая прозрачность и подотчетность: правовые подходы к разрешению проблемы «черного ящика». *Lex russica (Русский закон)*, *73*(6), 146. https://doi.org/10.17803/1729-5920.2020.163.6.139-148

Малышкин, А. В. (2019). Интегрирование искусственного интеллекта в общественную жизнь: некоторые этические и правовые проблемы. Вестник Санкт-Петербургского университета. *Право*, *10*(3), 444–460. https://doi.org/10.21638/spbu14.2019.303

Остроумов, Н. Н. (2015). *Правовой режим международных воздушных перевозок*. Москва: Статут. https://elibrary.ru/ulcfpl

[36] GDPR Privacy by Design. https://clck.ru/36h7vZ

Талапина, Э. В. (2020). Алгоритмы и искусственный интеллект сквозь призму прав человека. *Журнал российского права*, *10*, 25–39. https://doi.org/10.12737/jrl.2020.118

Akter, Sh., Dwivedi, Y. K., Sajib, Sh., Biswas, K., Bandara, R. J., & Michael, K. (2022). Algorithmic bias in machine learning-based marketing models. *Journal of Business Research*, *144*, 201–216. https://doi.org/10.1016/j.jbusres.2022.01.083

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, *159*, 107197. https://doi.org/10.1016/j.infsof.2023.107197

Bolton, M., Raven, R., & Mintrom, M. (2021). Can AI transform public decision-making for sustainable development? An exploration of critical earth system governance questions. *Earth System Governance*, *9*, 100116. https://doi.org/10.1016/j.esg.2021.100116

Bujold, A., Parent-Rocheleau, X., & Gaudet, M.-C. (2022). Opacity behind the wheel: The relationship between transparency of algorithmic management, justice perception, and intention to quit among truck drivers. *Computers in Human Behavior Reports*, *8*, 100245. https://doi.org/10.1016/j.chbr.2022.100245

Carlsson, V., & Rönnblom, M. (2022). From politics to ethics: Transformations in EU policies on digital technology. *Technology in Society*, *71*, 102145. https://doi.org/10.1016/j.techsoc.2022.102145

Cui, M., Mariani, M. S., & Medo, M. (2022). Algorithmic bias amplification via temporal effects: The case of PageRank in evolving networks. *Communications in Nonlinear Science and Numerical Simulation*, *104*, 106029. https://doi.org/10.1016/j.cnsns.2021.106029

Custers, B., & Heijne, A.-S. (2022). The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice. *Computer Law & Security Review*, *46*, 105727. https://doi.org/10.1016/j.clsr.2022.105727

de Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. *Government Information Quarterly*, *39*(2), 101666. https://doi.org/10.1016/j.giq.2021.101666

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988. https://doi.org/10.1016/j.telpol.2020.101988

Gordon, G., Rieder, B., & Sileno, G. (2022). On mapping values in AI Governance. *Computer Law & Security Review*, *46*, 105712. https://doi.org/10.1016/j.clsr.2022.105712

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, *45*, 105681. https://doi.org/10.1016/j.clsr.2022.105681

Kempeneer, Sh. (2021). A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. *Government Information Quarterly*, *38*(3), 101578. https://doi.org/10.1016/j.giq.2021.101578

Kempeneer, Sh., Pirannejad, A., & Wolswinkel, J. (2023). Open government data from a legal perspective: An AI-driven systematic literature review. *Government Information Quarterly*, 101823. https://doi.org/10.1016/j.giq.2023.101823

Lang, H., & Shan, C. (2000). Bias phenomenon and compensation in multiple target tracking algorithms. *Mathematical and Computer Modelling*, *31*(8–9), 147–165. https://doi.org/10.1016/S0895-7177(00)00063-7

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Li, Z. (2022). Affinity-based algorithmic pricing: A dilemma for EU data protection law. *Computer Law & Security Review*, *46*, 105705. https://doi.org/10.1016/j.clsr.2022.105705

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Mourby, M., Ó Cathaoir, K., & Bjerre Collin, C. (2021). Transparency of machine-learning in healthcare: The GDPR & European health law. *Computer Law & Security Review*, *43*, 105611. https://doi.org/10.1016/j.clsr.2021.105611

Qiaochu, W., Yan, H., Stefanus, J., & Param Vir, S. (2020, July 15). *Algorithmic Transparency with Strategic Users*. http://dx.doi.org/10.2139/ssrn.3652656

Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society*, *63*, 101421. https://doi.org/10.1016/j.techsoc.2020.101421

Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence:

Protecting fundamental rights and ethical values. *Computer Law & Security Review*, *45*, 105661. https://doi.org/10.1016/j.clsr.2022.105661

Stefik, M. (1996). Letting loose the light: Igniting commerce in electronic publication. In M. Stefik (Ed.), *Internet dreams: Archetypes, myths, and metaphors* (pp. 219–253). Cambridge, MA: MIT Press.

Stöger, K., Schneeberger, D., Kieseberg, P., & Holzinger, A. (2021). Legal aspects of data cleansing in medical AI. *Computer Law & Security Review*, *42*, 105587. https://doi.org/10.1016/j.clsr.2021.105587

Su, Zh., Bentley, B. L., McDonnell, D., Cheshmehzangi, A., Ahmad, J., Šegalo, S., Pereira da Veiga, C., & Xiang, Yu-Tao. (2023). China's algorithmic regulations: Public-facing communication is needed. *Health Policy and Technology*, *12*(1), 100719. https://doi.org/10.1016/j.hlpt.2022.100719

Varsha, P. S. (2023). How can we manage biases in artificial intelligence systems – A systematic literature review. *International Journal of Information Management Data Insights*, *3*(1), 100165. https://doi.org/10.1016/j.jjimei.2023.100165

Wang, H. (2022). Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency. *Philosophy & Technology*, *35*, 69. https://doi.org/10.1007/s13347-022-00564-w

Willems, J., Schmidthuber, L., Vogel, D., Ebinger, F., & Vanderelst, D. (2022). Ethics of robotized public services: The role of robot design and its actions. *Government Information Quarterly*, *39*(2), 101683. https://doi.org/10.1016/j.giq.2022.101683

Xu, J., Xiao, Yu., Wang, W. Hu., Ning, Yu., Shenkman, E. A., Bian, J., & Wang, F. (2022). Algorithmic fairness in computational medicine. *eBioMedicine*, *84*, 104250. https://doi.org/10.1016/j.ebiom.2022.104250

Zharova, A. (2019). Ensuring the information security of information communication technology users in Russia. *International Journal of Cyber Criminology*, *13*(2), 255–269. EDN: https://elibrary.ru/ltmesv. DOI: https://doi.org/10.5281/zenodo.3698141

Zharova, A. (2020). The protect mobile user data in Russia. *International Journal of Electrical and Computer Engineering*, *10*(3), 3184–3192. EDN: https://www.elibrary.ru/juzboh. DOI: https://doi.org/10.11591/ijece.v10i3.pp3184-3192

Zhu, H., Sallnäs Pysander, E.-L., & Söderberg, I.-L. (2023). Not transparent and incomprehensible: A qualitative user study of an AI-empowered financial advisory system. *Data and Information Management*, 100041. https://doi.org/10.1016/j.dim.2023.100041

Сведения об авторе

Жарова Анна Константиновна – доктор юридических наук, доцент, старший научный сотрудник, Институт государства и права Российской академии наук
Адрес: 420100, Российская Федерация, г. Москва, ул. Знаменка, 10
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56964137900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-4012-2015
Google Scholar ID: https://scholar.google.com/citations?user=g8ij3BsAAAAJ
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=151076

Конфликт интересов

Автор является главным редактором журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 22 мая 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.42

Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches

Anna K. Zharova

Institute of State and Law of the Russian Academy of Sciences
Moscow, Russian Federation

Keywords

algorithmic transparency,
artificial intelligence,
confidentiality,
data protection,
data security,
digital technologies,
GDPR,
information technologies,
law,
personal data

Abstract

Objective: to compare modern approaches in law to the use of program codes and algorithms in decision-making that meet the principles of transparency and openness, as well as the increasingly stringent requirements for ensuring the security of personal and other big data obtained and processed algorithmically.

Methods: the main methods for researching the principle of transparency in algorithmic decision-making were formal-legal and comparative analysis of legal acts and international standards of information security, as well as the principles and legal constructions contained in them.

Results: it was determined that the development of information security standardization, inclusion in legal acts of requirements for the development of information technologies that comply with the principles of transparency and openness of applied algorithms will minimize the risks associated with the unlawful processing of users' big data and obtaining information about their privacy. Proposals were identified, related to the implementation of algorithmic transparency in the field of data processing legal regulation. Recommendations were formulated, based on which the legislator can solve the problem of ensuring the openness of the logic of information technology algorithms with regard to modern standards of information security.

Scientific novelty: it consists in the substantiation of new trends and relevant legal approaches, which allow revealing the logic of data processing by digital and information technologies, based on the characterization of European standards of the "privacy by design" concept in new digital and information technologies of decision-making and data protection, as well as on the new legal requirements for artificial intelligence systems, including the requirement to ensure algorithmic transparency, and criteria for personal data and users' big data processing. This said, data protection is understood as a system of legal, technical and organizational principles aimed at ensuring personal data confidentiality.

Practical significance: it is due to the need to study the best Russian and international practices in protecting the privacy of users of digital and information technologies, as well as the need for legislative provision of requirements for the use of algorithms that meet the principles of transparency and openness of personal data processing, taking into account the need to ensure confidentiality at all stages of the life cycle of their processing, which will ensure the continuity of security management.

For citation

Zharova, A. K. (2023). Achieving Algorithmic Transparency and Managing Risks of Data Security when Making Decisions without Human Interference: Legal Approaches. *Journal of Digital Technologies and Law, 1*(4), 973–993. https://doi.org/10.21202/jdtl.2023.42

References

Akter, Sh., Dwivedi, Y. K., Sajib, Sh., Biswas, K., Bandara, R. J., & Michael, K. (2022). Algorithmic bias in machine learning-based marketing models. *Journal of Business Research*, *144*, 201–216. https://doi.org/10.1016/j.jbusres.2022.01.083

Balasubramaniam, N., Kauppinen, M., Rannisto, A., Hiekkanen, K., & Kujala, S. (2023). Transparency and explainability of AI systems: From ethical guidelines to requirements. *Information and Software Technology*, *159*, 107197. https://doi.org/10.1016/j.infsof.2023.107197

Bolton, M., Raven, R., & Mintrom, M. (2021). Can AI transform public decision-making for sustainable development? An exploration of critical earth system governance questions. *Earth System Governance*, *9*, 100116. https://doi.org/10.1016/j.esg.2021.100116

Bujold, A., Parent-Rocheleau, X., & Gaudet, M.-C. (2022). Opacity behind the wheel: The relationship between transparency of algorithmic management, justice perception, and intention to quit among truck drivers. *Computers in Human Behavior Reports*, *8*, 100245. https://doi.org/10.1016/j.chbr.2022.100245

Carlsson, V., & Rönnblom, M. (2022). From politics to ethics: Transformations in EU policies on digital technology. *Technology in Society*, *71*, 102145. https://doi.org/10.1016/j.techsoc.2022.102145

Cui, M., Mariani, M. S., & Medo, M. (2022). Algorithmic bias amplification via temporal effects: The case of PageRank in evolving networks. *Communications in Nonlinear Science and Numerical Simulation*, *104*, 106029. https://doi.org/10.1016/j.cnsns.2021.106029

Custers, B., & Heijne, A.-S. (2022). The right of access in automated decision-making: The scope of article 15(1)(h) GDPR in theory and practice. *Computer Law & Security Review*, *46*, 105727. https://doi.org/10.1016/j.clsr.2022.105727

de Bruijn, H., Warnier, M., & Janssen, M. (2022). The perils and pitfalls of explainable AI: Strategies for explaining algorithmic decision-making. *Government Information Quarterly*, *39*(2), 101666. https://doi.org/10.1016/j.giq.2021.101666

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6), 101988. https://doi.org/10.1016/j.telpol.2020.101988

Gordon, G., Rieder, B., & Sileno, G. (2022). On mapping values in AI Governance. *Computer Law & Security Review*, *46*, 105712. https://doi.org/10.1016/j.clsr.2022.105712

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, *45*, 105681. https://doi.org/10.1016/j.clsr.2022.105681

Gulemin, A. (2022). Limits of big data processing for the purposes of obtaining information about a person: a legal aspect. In Elektronnoe prilozhenie k "Rossiiskomu yuridicheskomu zhurnalu", 6, 52–57. (In Russ.). http://doi.org/10.34076/22196838_2022_6_52

Kempeneer, Sh. (2021). A big data state of mind: Epistemological challenges to accountability and transparency in data-driven regulation. *Government Information Quarterly*, *38*(3), 101578. https://doi.org/10.1016/j.giq.2021.101578

Kempeneer, Sh., Pirannejad, A., & Wolswinkel, J. (2023). Open government data from a legal perspective: An AI-driven systematic literature review. *Government Information Quarterly*, 101823. https://doi.org/10.1016/j.giq.2023.101823

Kuteynikov, D. L., Izhaev, O. A., Zenin, S. S., & Lebedev, V. A. (2020). Algorithmic transparency and accountability: legal approaches to solving the "black box" problem. *Lex russica*, *73*(6), 139–148. (In Russ.). https://doi.org/10.17803/1729-5920.2020.163.6.139-148

Lang, H., & Shan, C. (2000). Bias phenomenon and compensation in multiple target tracking algorithms. *Mathematical and Computer Modelling*, *31*(8–9), 147–165. https://doi.org/10.1016/S0895-7177(00)00063-7

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law & Security Review*, *48*, 105790. https://doi.org/10.1016/j.clsr.2023.105790

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Li, Z. (2022). Affinity-based algorithmic pricing: A dilemma for EU data protection law. *Computer Law & Security Review*, *46*, 105705. https://doi.org/10.1016/j.clsr.2022.105705

Malyshkin, A. V. (2019). Integration of artificial intelligence into public life: some ethical and legal problems. *Vestnik of Saint Petersburg University. Law*, *10*(3), 444–460. (In Russ.). https://doi.org/10.21638/spbu14.2019.303

Matheus, R., Janssen, M., & Janowski, T. (2021). Design principles for creating digital transparency in government. *Government Information Quarterly*, *38*(1), 101550. https://doi.org/10.1016/j.giq.2020.101550

Mourby, M., Ó Cathaoir, K., & Bjerre Collin, C. (2021). Transparency of machine-learning in healthcare: The GDPR & European health law. *Computer Law & Security Review*, *43*, 105611. https://doi.org/10.1016/j.clsr.2021.105611

Ostroumov, N. N. (2015). Legal regime of international air transportation. Moscow: Statut. (In Russ.).

Qiaochu, W., Yan, H., Stefanus, J., & Param Vir, S. (2020, July 15). *Algorithmic Transparency with Strategic Users*. http://dx.doi.org/10.2139/ssrn.3652656

Robinson, S. C. (2020). Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). *Technology in Society*, *63*, 101421. https://doi.org/10.1016/j.techsoc.2020.101421

Stahl, B. C., Rodrigues, R., Santiago, N., & Macnish, K. (2022). A European Agency for Artificial Intelligence: Protecting fundamental rights and ethical values. *Computer Law & Security Review*, *45*, 105661. https://doi.org/10.1016/j.clsr.2022.105661

Stefik, M. (1996). Letting loose the light: Igniting commerce in electronic publication. In M. Stefik (Ed.), *Internet dreams: Archetypes, myths, and metaphors* (pp. 219–253). Cambridge, MA: MIT Press.

Stöger, K., Schneeberger, D., Kieseberg, P., & Holzinger, A. (2021). Legal aspects of data cleansing in medical AI. *Computer Law & Security Review*, *42*, 105587. https://doi.org/10.1016/j.clsr.2021.105587

Su, Zh., Bentley, B. L., McDonnell, D., Cheshmehzangi, A., Ahmad, J., Šegalo, S., Pereira da Veiga, C., & Xiang, Yu-Tao. (2023). China's algorithmic regulations: Public-facing communication is needed. *Health Policy and Technology*, *12*(1), 100719. https://doi.org/10.1016/j.hlpt.2022.100719

Talapina, E. V. (2020). Algorithms and artificial intelligence in the human rights context. *Journal of Russian Law*, *10*, 25–39. (In Russ.). https://doi.org/10.12737/jrl.2020.118.

Varsha, P. S. (2023). How can we manage biases in artificial intelligence systems – A systematic literature review. *International Journal of Information Management Data Insights*, *3*(1), 100165. https://doi.org/10.1016/j.jjimei.2023.100165

Wang, H. (2022). Transparency as Manipulation? Uncovering the Disciplinary Power of Algorithmic Transparency. *Philosophy & Technology*, *35*, 69. https://doi.org/10.1007/s13347-022-00564-w

Willems, J., Schmidthuber, L., Vogel, D., Ebinger, F., & Vanderelst, D. (2022). Ethics of robotized public services: The role of robot design and its actions. *Government Information Quarterly*, *39*(2), 101683. https://doi.org/10.1016/j.giq.2022.101683

Xu, J., Xiao, Yu., Wang, W. Hu., Ning, Yu., Shenkman, E. A., Bian, J., & Wang, F. (2022). Algorithmic fairness in computational medicine. *eBioMedicine*, *84*, 104250. https://doi.org/10.1016/j.ebiom.2022.104250

Zharova, A. (2019). Ensuring the information security of information communication technology users in Russia. *International Journal of Cyber Criminology*, *13*(2), 255–269. DOI: https://doi.org/10.5281/zenodo.3698141

Zharova, A. (2020). The protect mobile user data in Russia. *International Journal of Electrical and Computer Engineering*, *10*(3), 3184–3192. https://doi.org/10.11591/ijece.v10i3.pp3184-3192

Zhu, H., Sallnäs Pysander, E.-L., & Söderberg, I.-L. (2023). Not transparent and incomprehensible: A qualitative user study of an AI-empowered financial advisory system. *Data and Information Management*, 100041. https://doi.org/10.1016/j.dim.2023.100041

Author information

Anna K. Zharova – Dr. Sci. (Law), Associate Professor, Senior Researcher, Institute of State and Law of the Russian Academy of Sciences
Address: 10 Znamenka Str., 420100 Moscow, Russian Federation
E-mail: anna_jarova@mail.ru
ORCID ID: https://orcid.org/0000-0002-2981-3369
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56964137900
WoS Researcher ID: https://www.webofscience.com/wos/author/record/H-4012-2015
Google Scholar ID: https://scholar.google.com/citations?user=g8ij3BsAAAAJ
RSCI Author ID: https://elibrary.ru/author_items.asp?authorid=151076

Conflict of interest

The author is an Editor-in-Chief of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research was not sponsored.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 22, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:343.3/.7:341.4:343.9
EDN: https://elibrary.ru/cmvqzx
DOI: https://doi.org/10.21202/jdtl.2023.43

Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре
г. Сохаг, Египет

Ключевые слова

кибербезопасность,
киберпространство,
кибертерроризм,
международное публичное право,
международное частное право,
права человека,
право,
преступления против человечности,
цифровые технологии,
юрисдикция

Аннотация

Цель: развитие беспроводных технологий и цифровой инфраструктуры радикальным образом изменило среду обитания человечества, порождая новый тип пространства – киберпространство. Уникальность и особенности этой среды, включая анонимность, безграничность, проблемы, связанные с определением и установлением юрисдикции, стали питательной средой для появления новой глобальной угрозы – кибертерроризма, характеризующегося высоким уровнем латентности, низким уровнем раскрываемости и несравнимо большей опасностью, нежели преступления «в реальном мире». Противодействие новым формам преступности потребовало разработки универсальных инструментов, преодолевающих ограничения традиционной юрисдикции и позволяющих государствам преследовать террористов в киберпространстве. Определение соответствующих инструментов и выявление препятствий политико-юридического характера по их реализации является целью проведенного исследования.

Методы: для достижения поставленной цели используется, прежде всего, формально-юридический метод, применяемый для анализа правовых источников, к которым относятся судебная практика, национальное законодательство и международные акты. Также был задействован доктринальный подход, позволивший на основе научных трудов и теоретических конструкций объяснить сложность новых явлений современного мира и спрогнозировать их развитие в будущем. Основное внимание при этом уделяется стороне преступника, чтобы доказать ее антагонизм с человечеством в соответствии с теоретическими взглядами. Наконец, в исследовании анализируются теории универсальной и традиционной юрисдикции, а также то, как они применяются для преследования террористов.

Результаты: в работе дается критический анализ переосмысления и адаптации концепции юрисдикции применительно к глобальной, безграничной и децентрализованной цифровой среде (киберпространство) и противодействию новым формам терроризма (кибертерроризм); приводятся различные юрисдикционные модели, применимые в киберпространстве; преодолевается разрыв между основными отраслями права: международным частным и публичным правом – путем установления взаимосвязи в отношении к кибертерроризму двух теорий: концепций «обязанности защищать» (R2P) и применения универсальной юрисдикции; выявлены тенденции развития универсальной юрисдикции.

Научная новизна: исследование развивает накопленные научные знания в части обоснования введения иностранной юрисдикции на территории государства для преследования кибертеррористов; устанавливается связь между теориями универсальной юрисдикции в международном частном праве и «обязанностью защищать» (R2P) в международном публичном праве; при этом последняя признается в качестве пригодной основы для введения универсальной юрисдикции в отношении кибертерроризма; переосмысливаются такие традиционные понятия, как суверенитет и юрисдикционная независимость. Устраняется пробел в знаниях, связанных с рассмотрением кибертерроризма как преступления против человечности в международном праве.

Практическая значимость: реализация предложенных выводов будет способствовать усилению международного преследования кибертерроризма; гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления.

Для цитирования

Абделькарим, Я. А. (2023). Применение концепции «обязанность защищать» (R2P) для введения универсальной юрисдикции в отношении кибертерроризма. *Journal of Digital Technologies and Law*, *1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

Содержание

Введение

Ученые всего мира признают, что концепция «обязанность защищать» предусматривает необходимость защиты прав человека. Кроме того, не вызывает сомнений глобальный характер потенциальных разрушений в результате кибертерроризма. Следовательно, упомянутая теория является адекватным основанием для введения универсальной юрисдикции в отношении кибертерроризма. В настоящей статье представлена концепция «обязанность защищать» (англ. “responsibility to protect”, далее – R2P), которая обосновывает введение универсальной юрисдикции в отношении кибертерроризма. Автор показывает связь между двумя теориями международного права: теорией универсальной юрисдикции в рамках международного частного права и концепцией «обязанность защищать» в рамках международного публичного права.

Исследование вносит вклад в науку, предлагая международному сообществу правовое обоснование введения иностранной юрисдикции на территории государства для преследования кибертеррористов. Установлена связь между теорией универсальной юрисдикции в международном частном праве и концепцией «обязанность защищать» в международном публичном праве. Таким образом, преодолевается разрыв между этими основными отраслями международного права. Кроме того, работа задает новый контекст традиционным понятиям, например, понятиям суверенитета и юрисдикционной независимости, для достижения ранее поставленных целей гуманитарных наук. Исследование также устраняет пробел в науке, связывая кибертерроризм с известной в международном праве концепцией преступлений против человечности (далее – ППЧ); автор доказывает применимость элементов последней к кибертерроризму как международной противоправной деятельности. Таким образом, теория R2P может способствовать установлению универсальной юрисдикции в отношении кибертерроризма, как это происходит в отношении ППЧ.

В работе анализируется структура кибертерроризма и исследуются его скрытые элементы в условиях неоднозначности киберпространства. Безграничность последнего требует разработки инструмента, преодолевающего ограничения традиционной юрисдикции. Таким инструментом является универсальная юрисдикция, позволяющая государствам преследовать террористов в киберпространстве независимо от их местонахождения. Однако ее применение наталкивается на препятствия как юридического, так и политического характера. Поэтому эффективным средством поддержки этого инструмента должна стать теория, включающая ряд обязательных элементов.

Проведенное исследование должно поспособствовать развитию уголовного преследования кибертерроризма во всем мире, поскольку обосновывает использование международного правового инструментария против этого преступления. Доказывается, что кибертерроризм – это преступление против человечности, требующее международного вмешательства в соответствии с теорией R2P, которая представлена как регулятивная правовая норма. Автор показывает необходимость для всех стран сплотиться ради предотвращения этих тяжких преступлений в соответствии

с нормами Устава ООН путем гармонизации международного и внутригосударственного правового инструментария в отношении данного преступления. Таким образом, международное право способно выступить против кибертерроризма и искоренить его в киберпространстве.

Методология. Для достижения поставленных целей в исследовании использован теоретический подход. Он основан на доктринальном методе изучения первичных и вторичных источников права с целью анализа встречающихся в них положений. К таким источникам относятся судебная практика, внутреннее законодательство стран и международные правовые акты. Анализ основывается на логических рассуждениях. При таком подходе анализируются нормы, включенные в правовые материалы для выработки правового понимания вопроса исследования. Кроме того, изучены аргументированные обзоры судебной практики и первичных правовых источников.

Обзор научных публикаций по теме позволяет выявить пробелы в знаниях, на устранение которых и направлено исследование. Рассматривается контекст теории R2P, подчеркивается ее цель – защита человечества от преступлений. Далее в работе рассматривается концепция кибертерроризма и доказывается антагонизм преступника по отношению к человечеству. Наконец, в исследовании подвергается критике имеющаяся в литературе информация о теории универсальной юрисдикции и о том, как она применяется для преследования террористов в различных юрисдикциях.

Кроме того, проанализированы источники международного и национального права с целью изучения того, как теория универсальной юрисдикции используется при преследовании кибертеррористов. В статье описаны соответствующие тенденции в отношении данной теории.

1. Превентивный характер концепции «обязанность защищать» (R2P) в отношении преступлений против человечности (ППЧ)

В международном праве постулируется безусловная обязанность государств защищать человечество от злодеяний. Международный пакт о гражданских и политических правах и Международный пакт об экономических, социальных и культурных правах указывают основные права человека в качестве объекта такой защиты. Еще в 1948 г. была принята Конвенция о предупреждении преступления геноцида и наказании за него, установившая обязанность государства предотвращать преступления, связанные с геноцидом[1]. Кроме того, эти обязанности закреплены в Уставе ООН в целях защиты человечества путем обеспечения мира во всем мире. Постепенно эта доктрина ООН стала восприниматься как защита от ППЧ[2]. В докладе Всемирного саммита 2005 г. четко обозначено, что теория ответственности международного сообщества необходима для достижения целей ООН. Указанные правовые инструменты устанавливают пороговые показатели возникновения обязательств государства. Юридическая сила этих обязательств отражает возможности их соблюдения в рамках глобальной правовой системы и решимость государств защищать человечество. Таким образом, концепция «обязанности защищать» имеет прочные корни в международном праве.

1 The 1948 Convention on the Prevention and Punishment of the Crime of Genocide, Arts 3, 6 and 8.

2 The UN General Assembly. Resolution Adopted by the General Assembly: 60/1 (UN, 2005), para. 139 and the Resolution A/75/277 (UN 2021), para. 6.

1.1. Унификация концепции R2P для предотвращения ППЧ

Таким образом, доктрина устанавливает концепцию R2P в качестве международно-правовой нормы, направленной на предотвращение бесчеловечных злодеяний. Она упоминается в резолюциях Совета безопасности ООН (далее – СБ ООН) для обоснования вмешательства при предотвращении преступлений против человечности[3]. Такая позиция превращает концепцию R2P из некоей инновационной идеи в общепризнанный правовой принцип международного права. Появляется системная правовая основа для вмешательства при предотвращении ППЧ (Cantini & Zavialov, 2018). ППЧ подразумевают ответственность международного сообщества за принятие мер, независимо от соображений суверенитета. Таким образом, концепция R2P подразумевает содействие мерам по предотвращению преступлений против человечности, предпринимаемым международным сообществом или иностранной юрисдикцией (Cantini & Zavialov, 2018).

По утверждению Ч. Ройера, политическая воля государств и традиционное понимание их суверенитета препятствуют вмешательству международного сообщества для предотвращения ППЧ (Royer, 2021). Поэтому он подчеркивает, что при интерпретации своих национальных интересов в отношении преступлений против человечности государства должны задействовать концепцию R2P (Royer, 2021). По его мнению, концепция R2P не может служить ориентиром для государственной политики, поэтому страны часто выступают против его применения. Это предполагает переосмысление усилий международного сообщества по борьбе с преступлениями. При этом, хотя концепция R2P представляет собой моральную норму, в доктрине она должна рассматриваться как превентивная процедура для защиты человечества (Royer, 2021). Такая интеграция поддерживает роль концепции R2P в международной политике, поскольку исключает экстремистские патриотические настроения, направленные против иностранного вмешательства. Новое понимание концепции R2P, предложенное Ройером, подчеркивает серьезность ППЧ как всеобщего зла, для борьбы с которым необходимо сотрудничество на глобальном уровне.

По мнению С. Уатта, концепция R2P должна быть закреплена в международном праве посредством институтов ООН (Wyatt, 2019). Он утверждает, что данная концепция продолжает политику защиты человечности, принятой ООН, поскольку налагает на государства-члены коллективную ответственность за предотвращение преступлений против человечности (Wyatt, 2019). Кроме того, она расширяет пределы строгого понимания государственного суверенитета в духе Вестфальской системы[4], дополняя его с точки зрения ответственности. Таким образом, понятия суверенитета и космополитической защиты человечности оказываются связаны моралью. С. Уатт также считает, что органы ООН могут эффективно обеспечить соблюдение правопорядка в соответствии с концепцией R2P, поэтому именно они должны следить за ее применением. Такой конституционный порядок гарантирует эффективную интеграцию обязательств в рамках концепции R2P в международное право и их стабильное исполнение. В этом проявляется солидарная ответственность на глобальном уровне, заложенная в Уставе ООН. Тем самым международная дипломатия и доктрина получают сбалансированную концепцию всеобщей солидарности для поддержания мира

[3] Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

[4] Там же, p. 99. Суверенитет понимается как «высшая власть на определенной территории».

и безопасности[5]. Такая интерпретация направлена на закрепление концепции R2P в международном праве и дипломатии. Попытка навязать конституционный характер концепции R2P государствам требует их четкого согласия, поскольку может противоречить их трактовке суверенитета. Кроме того, упомянутый баланс подразумевает унификацию взглядов государств на их ответственность, иначе противодействие ППЧ будет рассматриваться как солидарное обязательство в рамках Устава. На практике политические круги противостоят попыткам применить концепцию R2P, считая ее проявлением западного империализма, которому следует оказывать сопротивление из патриотических соображений. Несмотря на то, что интервенция НАТО в Ливию была одобрена СБ ООН в соответствии с концепцией R2P[6], она подверглась критике, поскольку нарушила государственный суверенитет и привела к политическому хаосу в стране. Это может быть расценено как использование международного правосудия в политических целях. Чтобы решить эту проблему, в международном праве необходимо юридически контекстуализировать концепцию R2P для каждого конкретного случая, чтобы гарантировать ее непредвзятость.

ППЧ со стороны третьих лиц, например террористов, в отношении местного населения влечет за собой обязанность международного сообщества вмешаться с целью предотвращения преступления, если не последовало реакции государства, где это произошло (Soler, 2019). При таком внешнем вмешательстве могут использоваться инструменты иностранной юрисдикции. Здесь объединяются обязанности как государства, так и международного сообщества по предотвращению жестоких злодеяний, нарушающих основные права человека (Park & Switzer, 2020), а правовые процедуры становятся транснациональными[7]. Таким образом, подобные вмешательства обеспечивают достижение целей концепции R2P, поскольку ее гуманитарные аспекты преобладают над соображениями суверенитета. Эта обязанность международного сообщества вызывается невыполнением соответствующим государством своих обязанностей по защите основных прав человека. Кроме того, преступления против человечности не должны использовать государственный суверенитет в качестве щита, позволяющего избежать судебного преследования (Soler, 2019). Более того, международное право допускает гуманитарное вмешательство для предотвращения нарушений прав человека даже с применением силы, хотя и в редких случаях (Azubuike, 2023). Обращение в суд тем более является подходящим решением для защиты этих прав. Эти права закреплены в международном праве, которое предоставляет им постоянную защиту.

Примечательно, что нормы R2P могут быть использованы в киберпространстве для пресечения террористической деятельности и содействовать сотрудничеству крупнейших интернет-компаний и государственных органов в обеспечении ответственных мер для достижения этой цели (Park & Switzer, 2020). Это подтверждает, что концепция R2P может помочь бороться с кибертерроризмом в киберпространстве.

---

5 Там же, p. 156.

6 The United Nations Security Council S/RES/1973 (2011), para. 4.

7 Kosiba, K. (2018). Is R2P the Remedy for Illegal Deforestation? A Case Study Based on the Systematic Human Rights Violations in Peru. Master of Arts Dissertation submitted to the Brussels School of International Law. University of Kent. https://clck.ru/36ksvy

1.2. Применение R2P в международном праве

Международный суд ООН определяет R2P как коллективную обязанность по поддержанию всеобщего мира и безопасности[8]. Таким образом, государства должны использовать доступные им методы для достижения этой цели. По своей сути концепция R2P представляет собой обязательство должной ответственности, поскольку государства не обязаны добиваться полного предотвращения этих преступлений[9]. Эта норма показывает гибкость концепции R2P в международном праве, что делает ее адекватным основанием для применения универсального инструментария, т. е. универсальной юрисдикции, в отношении ППЧ.

Установление ответственности за преступления против человечности расширяет повестку дня Международного уголовного суда (далее – МУС) по обеспечению эффективной защиты человека (Bellamy, 2018). На данном этапе концепция R2P соответствует целям Римского статута, поскольку может быть использована для обеспечения правовой основы инструментария МУС. Концепция использует невоенные превентивные меры МУС для пресечения ППЧ в соответствии со ст. 7 Статута (Holvoet & Mema, 2015). Действительно, МУС оказывается эффективным для достижения этой цели благодаря своим принципам превентивности и постоянства (Holvoet & Mema, 2015). Таким образом, комплексное использование инструментов МУС и R2P сможет эффективно защитить человечество от ППЧ.

Эта гуманитарная цель оправдывает использование данных инструментов даже в отношении государств, не являющихся сторонами Конвенции, особенно при закреплении R2P в резолюциях СБ ООН. Однако для обеспечения эффективности этого инструмента необходимо задействовать дипломатические и гуманитарные механизмы (Bellamy, 2018). Такой подход предполагает использование правового инструментария иностранных юрисдикций. Например, МУС ввел свою юрисдикцию в Кении и предъявил правительству страны ультиматум о создании специального суда по делам о насилии после выборов (Bellamy, 2018). Юридические меры Международного уголовного суда в данном случае опирались на концепцию R2P, поскольку были направлены на защиту местного населения от насилия. А. Беллами делает вывод о том, что и R2P, и система МУС являются комплексными гуманитарными институтами, призванными предотвратить ППЧ. Несмотря на скептическое отношение к невоенным мерам в рамках R2P, их реализация представляет собой альтернативу военным операциям (Fehl, 2015). Это промежуточная мера, способная предотвратить международные преступления, что делает бесспорным их огромное значение для человечества.

Хотя Международный уголовный суд и R2P совместно играют большую роль в предотвращении преступлений против человечности, использование универсального судебного инструментария должно быть подчинено целям Римского статута (Holvoet & Mema, 2015). Это условие гарантирует эффективность и надежность мер МУС в отношении ППЧ, поскольку обеспечивает судебный надзор за практикой Международного уголовного суда. Таким образом, этот механизм повышает доверие к роли МУС в противодействии преступлениям против человечности и борется

---

8 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

9 Там же.

с безнаказанностью преступников. Как отмечают исследователи, инструментарий R2P стоит на страже международного правосудия и безопасности, поскольку предусматривает международное вмешательство для обеспечения соблюдения международного права во всем мире (Ercan, 2022).

Подводя итог, можно сказать, что, согласно научным исследованиям и данным судебной практики, концепция R2P основывается на необходимости поддержания мира и безопасности. С этой точки зрения она представляет собой правовую норму, предусматривающую вмешательство в отношении серьезных ППЧ вне установленных юрисдикций. Таким образом, она является адекватным обоснованием для применения иностранных правовых норм, в частности универсальной юрисдикции, в государстве, где совершено преступление. Тем самым преодолеваются рамки суверенитета, которые могут препятствовать защите безопасности человека, что побуждает международное сообщество к выполнению своих обязанностей по защите человечности.

2. Правовые основы для отнесения кибертерроризма к категории «другие бесчеловечные деяния» согласно Римскому статуту

Не вызывает сомнений, что киберпространство устанавливает международные связи между отдельными государствами. В силу технической природы киберпространства террористы используют его преимущества для достижения своих целей. Это позволяет им избегать преследования со стороны национальных правоохранительных органов. Поэтому они действуют на глобальном уровне, угрожая миру во всем мире. Кибертерроризм – это сложившаяся система антигуманной деятельности, пресечение которой требует международно-правовых усилий.

Поддержание всеобщего мира и безопасности является одной из главных целей международных правовых органов, в частности Международного уголовного суда. В силу своих глобальных правовых возможностей он является компетентным органом для преследования международных преступников. Однако в Римском статуте, который его регулирует, говорится исключительно о деяниях, подпадающих под юрисдикцию суда. Кибертерроризм среди них не упоминается. Правда, в нем отмечается, что при определенных условиях юрисдикция суда распространяется и на неупомянутые бесчеловечные деяния[10].

В настоящей статье мы рассмотрим правовые основы, позволяющие расценивать кибертерроризм как преступление против человечности в соответствии с Римским статутом Международного уголовного суда. Степень вреда от этой деятельности достаточна для того, чтобы отнести ее к данной категории, что подводит ее под юрисдикцию МУС. В работе проводится анализ кибертерроризма и обзор литературы с целью выделения его основных элементов. Затем проводится реконцептуализация доктрины международного права о преступлениях против человечности с целью доказать применимость этой концепции к кибертерроризму. Теоретическая значимость исследования состоит в установлении правовых основ для распространения юрисдикции МУС на преследование кибертеррористов. Эта глобальная преступная деятельность требует глобального правового механизма для ее пресечения. Таким образом, международное сообщество сможет бороться с кибертерроризмом, укрепляя мир и безопасность во всем мире.

[10] The Rome Statute of the International Criminal Court (2002), Article 7 (1) (k), A/CONF.183/9.

2.1. Анализ кибертерроризма

В наш информационный век терроризм проник в киберпространство, создав новую угрозу для человечества. Кибертерроризм – это террористическое воздействие на группу лиц с политическими или радикальными целями с использованием Интернета (Broeders et al., 2021). Это особый вид терроризма, который следует анализировать с широкой точки зрения. Кибертеррористы используют возможности Интернета, который сложно контролировать. Французский словарь терминов национальной безопасности характеризует кибертерроризм через фактор риска, связанный с незаконной кибератакой (Delerue et al., 2019). С помощью Интернета террористические группы могут действовать на транснациональном уровне, преодолевая географические расстояния (Albahar, 2019), поэтому кибертерроризм нужно изучать в международном аспекте. Так, А. Перлофф-Джайлс характеризует кибертеррористов как «врагов человечества» (Perloff-Giles, 2018), проводя параллель между кибертерроризмом и пиратством, поскольку и та и другая деятельность угрожает интересам международной торговли. Исследователь подчеркивает, что в долгосрочной перспективе атаки кибертеррористов ставят под угрозу всю работу сети, что указывает на значительный вред этой деятельности. Кроме того, автор выделяет три признака транснациональных киберпреступлений:

– это преднамеренное действие, причиняющее вред невиновным лицам, например, преднамеренная атака на инфраструктуру страны, правительственные или частные компьютерные системы. Такое действие может быть совершено как государственным, так и негосударственным субъектом. К последней категории и относятся кибертеррористы.

– действие должно происходить в киберпространстве, что позволяет обеспечить анонимность и малозатратность атак,

– действие должно иметь транснациональный характер, поскольку преступники действуют, невзирая на национальные границы. Рассылаемые ими вредоносные программы пересекают границы без паспортов. Кроме того, последствия таких преступлений затрагивают несколько юрисдикций (Perloff-Giles, 2018).

Автор также утверждает, что кибератаки, кто бы их ни совершал, представляют собой незаконное применение силы, что влечет за собой право на самооборону в соответствии со ст. 51 Устава ООН. Это является основанием для применения международного гуманитарного права как релевантной правовой нормы для ликвидации последствий киберконфликтов. Однако для его применения необходимы следующие условия:

– серьезность и масштабность атак. Перлофф-Джайлс считает, что этот параметр должен позволять квалифицировать их как «вооруженное нападение»;

– идентификация исполнителей для установления их ответственности. При этом исследователь признает сложность определения такой идентификации в отношении киберпреступлений (Perloff-Giles, 2018).

Таким образом, исследователь указывает на значение киберпреступлений как уникальной формы агрессии. Эта деятельность, как и обычные вооруженные конфликты, должна приводить к применению международного гуманитарного права. Это означает, что кибертерроризм представляет собой серьезную угрозу человечеству, которая требует использования международных норм.

В книге «Определение международного терроризма» С. Маргарити утверждает, что терроризм угрожает интересам международного сообщества, ущемляя основные права человека, касающиеся всеобщей безопасности и мира (Margariti, 2017). В работе описана глобальная составляющая терроризма и показано, что его последствия выходят за пределы национальных границ и распространяются на все международное сообщество (Margariti, 2017). Поскольку киберпространство не связано с географическими границами государств, все возникающие в нем проблемы приобретают всеобщий характер. Преступные действия в киберпространстве также выходят за пределы границ стран. Следовательно, кибертерроризм неизбежно оказывает влияние на международную безопасность.

В силу отсутствия границ террористические группировки используют киберпространство для достижения своих целей. Известно, что такие организации, как ИГИЛ, используют социальные сети для запугивания путем трансляции видеоконтента. Кроме того, они используют эти сайты в качестве вербовочных площадок. Таким образом, они могут действовать в глобальном масштабе, невзирая на географические границы (Awan, 2017). Эта возможность дает террористам преимущество перед органами правопорядка и безопасности. Поэтому необходимо изучать кибертерроризм как самостоятельный вид преступной деятельности, сочетающий террор и технологии.

Так, В. Коррейя определяет кибертерроризм как «деятельность посредством кибернетических систем, направленную на продвижение политических, социальных или религиозных идеологий против населения, и деятельность, использующую киберсистемы, направленную на угрозу или содействие нанесению ущерба населению, имуществу и/или системам. Кибертерроризм может сочетаться с традиционным терроризмом» (Correia, 2022). Исследователь вводит понятие динамики кибертерроризма, отражающее его изменчивость. Кроме того, она требует ввести особое определение субъективной стороны преступления, которое относится к радикальным мотивам поведения. При этом уточняется, что физическое воздействие не является условием кибертерроризма – возможно нанесение вреда системам, не имеющим физической формы. Предполагается, что введение данного определения будет способствовать международному сотрудничеству в области уголовного преследования и противодействия кибертерроризму. Исследователь также указывает на влияние кибертерроризма на граждан внутри страны. Автор призывает учитывать проблему незаконного использования террористами технологий и изучать данную деятельность на основе комплексного подхода (Correia, 2022).

Напротив, понятие кибертерроризма не включает ненасильственные методы, так как, по определению, он должен приводить к ущербу независимо от его целей. По мнению А. Хеншке и соавторов, использование террористами Интернета для вербовки членов или распространения своих радикальных взглядов само по себе является лишь деятельностью по распространению угроз в адрес целевой аудитории (Henschke, 2021). Отсутствие физического ущерба не позволяет квалифицировать эту деятельность как кибертерроризм. Примечательно, что Хеншке признает, что кибератаки на устройства интернета вещей[11] могут привести к физическому воздействию на

[11] Интернет вещей – система, позволяющая управлять физическими устройствами посредством кодов искусственного интеллекта.

жертвы (Henschke, 2021). Таким образом, они представляют собой кибертерроризм, поскольку вмешиваются в установленную интернетом вещей связь между информационной сетью и физическим миром. Кроме того, по мнению ученых, в Таллиннском руководстве предусмотрено условие, что воздействие кибератаки в физическом мире должно быть ощутимо в той же мере, что и реальное применение силы (Schmitt, 2013). В Руководстве указано, что неразрушительные кибердействия не являются применением силы независимо от их моральных последствий (Schmitt, 2013).

По мнению Д. Броедерс, пока не было зафиксировано кибератак, причинивших физический ущерб (Broeders et al., 2021). Он утверждает, что террористы не обладают необходимыми техническими и финансовыми навыками для совершения кибератак. Кроме того, законодательство Великобритании требует применения насилия для признания акта «террористическим»[12], что исключает ненасильственные действия такого рода. В этой связи К. Стоддарт подчеркивает, что кибертерроризм угрожает инфраструктуре США, поскольку может затронуть деятельность государства. Кроме того, кибертерроризмом можно считать шпионскую деятельность, хотя она может и не носить насильственного характера, что еще раз подчеркивает серьезность проблемы (Stoddart, 2022).

Эти взгляды отражают лишь самый поверхностный анализ кибертерроризма, поскольку не учитывают того факта, что моральные последствия этой деятельности превосходят физический ущерб от нее. Деморализация страны в результате кибертерроризма приводит к опасным экономическим и социальным последствиям. Кибертерроризм порождает гнев среди населения, ставшего объектом нападения, что побуждает его требовать возмездия в виде применения силы (Shandler et al., 2021) и политического ответа, как и в случае обычного терроризма (Shandler et al., 2021). Кроме того, оба вида терроризма мотивируются одними и теми же психологическими стимулами.

По мнению Королевской уголовной прокуратуры (Великобритания), чтобы действия были признаны террористическими, они должны быть мотивированы террором[13]. Аналогичным образом, принятый в Египте Закон о борьбе с терроризмом предусматривает, что даже психологические угрозы невинным людям представляют собой террористический акт, независимо от нанесенного им физического ущерба[14]. В соответствии с этим законом, намерение терроризировать гражданское население для реализации целей преступников является достаточным для признания их действий преступными. Таким образом, национальные законодательства отдают приоритет соображениям безопасности, игнорируя условие физического воздействия, которого требует А. Хеншке (Henschke, 2021). Кроме того, в Единой позиции 2001/931/CFSP атаки на национальную инфраструктуру или государственные объекты рассматриваются как террористические акты, в связи с чем к виновным применяются контртеррористические меры[15]. Принятая в Австрии Стратегия кибербезопасности

12 The Terrorism Act 2006, c. 11. https://clck.ru/34Chci

13 The Crown Prosecution Service. (2021). Terrorism. https://clck.ru/36kt3Z

14 Law No 94/2015, art 2 para 1.

15 Article 1(3) of Common Position 2001/931/CFSP, см. The EU list of persons, groups and entities subject to specific measures to combat terrorism, Factsheet on 14 January 2015. https://clck.ru/36kt4j

для квалификации акта в качестве террористического также требует наличия намерения терроризировать гражданское население с целью нанесения ущерба инфраструктуре или экономике страны[16]. Таким образом, в законодательстве многих стран внимание концентрируется на психологическом аспекте терроризма, поскольку именно намерение запугать невиновных относит преступное деяние к данной категории. Именно этот отличительный элемент кибертерроризма, который может не причинить физического ущерба, и является определяющим фактором данной категории.

Аналогичным образом С. Маргарити утверждает, что намерение запугать квалифицирует деяние как террористическое, независимо от его мотивов (Margariti, 2017). Этот элемент отличает терроризм от обычных преступлений. Это та специфическая субъективная сторона преступления, которая определяет его классификацию. Исследователь принимает этот стандарт в качестве всеобщего детерминанта объективной стороны международного терроризма, необходимого для применения к нему универсальных правовых норм (Margariti, 2017).

Таким образом, необязательность физического воздействия для признания акта террористическим усиливает инклюзивную тематику исследований кибертерроризма, что согласуется с определением В. Коррейя, рассмотренным выше (Correia, 2022). Даже имея только моральные последствия, кибертерроризм угрожает всеобщему миру и безопасности, так как может привести к вооруженному конфликту. В отличие от обычного терроризма люди не могут укрыться от кибертерроризма; коды, которые используют кибертеррористы для нанесения ущерба вычислительным системам целевой аудитории, проникают через многочисленные уровни защиты. Таким образом, отсутствие кибербезопасности дестабилизирует мир и безопасность во всем мире. Кибертерроризм может быть возведен в ранг врага человечества, как это предлагает А. Перлофф-Джайлс (Perloff-Giles, 2018).

2.2. Контекстуальные элементы преступлений против человечности: другие бесчеловечные деяния

Статья 7(1)(k) Римского статута включает термин «другие бесчеловечные деяния» для установления юрисдикции МУС в отношении этих тяжких деяний. Этот термин прочно вошел как в доктрину, так и в судебную практику. Однако для целей настоящей работы мы рассмотрим элементы этого понятия, чтобы сравнить их и доказать его применимость к кибертерроризму как международной противоправной деятельности. Поскольку данный термин был сформулирован в рамках международного права, необходимо изучить его элементы с точки зрения международной доктрины и судебной практики.

Изначально ст. 7(1)(k) Статута устанавливает, что категория «другие бесчеловечные деяния» является неотъемлемой частью ППЧ, запрещенных Статутом (Broeders et al., 2021). В статье перечислены следующие элементы этого деяния, аналогичные основным элементам преступлений против человечности: бесчеловечные действия, намерения причинить психологические или физические страдания. Однако данное определение шире, чем определение ППЧ, чтобы дать возможность преследовать деяния, не включенные в преступления против человечности.

---

16 Federal Chancellery of the Republic of Austria. (2013). Austrian Cyber Security Strategy. Vienna. https://clck.ru/36kt6E

В работе Р. Атаджанова утверждается, что системный характер преступлений против человечности отличает их от обычного преступного поведения (Atadjanov, 2019). Таким образом, организованность поведения отражает элемент контекста, необходимый для квалификации деяния в качестве преступления против человечности. Именно эта организованность позволила Гоббсу утверждать, что ППЧ выражают «крайнюю степень зла» (Hobbs, 2017). Таким образом, этот элемент отражает их масштабность и тяжесть для законных интересов человечества. Однако, по мнению Сеада Хусейн Адема, понятие ППЧ страдает от нормативного пробела в международной доктрине, который Статут стремится восполнить путем перечисления элементов, квалифицирующих деяние как преступление против человечности (Adem, 2019). Исследователь приходит к выводу, что судебная практика по делам о преступлениях против человечности также помогает устранить этот пробел, поскольку специальные трибуналы и Международный уголовный суд разработали инклюзивный подход, который разрешил эту дилемму (Adem, 2019).

Комиссия по международному праву (далее – КМП) требует, чтобы подобные деяния и их последствия рассматривались как ППЧ[17]. Кроме того, утверждается, что они могут быть совершены негосударственными субъектами[18]. Поэтому КМП допускает классификацию деяний, совершенных группами или организациями, в качестве ППЧ в соответствии с положениями Римского статута. По мнению Комиссии, преступления против человечности могут совершаться не только государствами, но и независимыми структурами или отдельными лицами. Кроме того, основным элементом данного преступления КМП считает многочисленность жертв. Это условие не позволяет отнести отдельные ограниченные деяния к данной категории.

Что касается судебной практики, то термин «бесчеловечные деяния» отражает развитие классификации преступлений против человечности. Этот поход использовался в 18 делах, рассмотренных МУС, в качестве альтернативного ответа на правовой вакуум (MacNeil, 2021). В деле Prosecutor v Jean-Pierre Bemba Gombo[19] утверждается, что преступления против человечности имеют четыре составляющих: нацеленность на гражданских лиц, масштабность, совершенные действия, субъективную сторону[20]. Кроме того, Международный уголовный суд считает преступлениями против человечности бесчеловечные действия, причиняющие психологический ущерб[21]. В деле Prosecutor v Germain Katanga и Mathieu Ngudjolo Chui[22] суд постановил, что серьезные нарушения основных прав человека, закрепленных в международном праве, являются бесчеловечными деяниями в соответствии со ст. 7(1)(k) Статута[23].

---

17 The International Law Commission, Draft Code of Crimes against the Peace and Security of Mankind, 1996 UN Doc. A/51/10 article 18 (k), c. 47. https://clck.ru/36kt7d

18 Там же.

19 Case No. ICC-01/05-01/08.

20 Там же, para 117 и (Park & Switzer, 2020).

21 Там же. Также см. International Criminal Court. (2013). Elements of Crimes. ISBN 92-9227-232-2, ICC-PIOS-LT-03-002/15_Eng. https://clck.ru/36ktC8

22 Case No. ICC-01/04-01/07.

23 Там же, para 448. МУС применил тот же принцип в запросе The Request for authorization of an investigation pursuant to article 15 относительно ситуации в Бангладеш и Республике Союза Мьянма, Case No. ICC-01/19, para 128.

Как отмечает Дж. Куигли, по классификации МУС контекстуальными элементами категории «другие бесчеловечные деяния» является преднамеренное причинение сильных страданий или психологического или физического вреда (Quigley, 2023). По мнению ученого, это самостоятельная категория уголовного права, не требующая установления связи с другими включенными преступлениями (Quigley, 2023).

Международным уголовным трибуналом по бывшей Югославии (далее – МТБЮ) было принято решение, что действия, ущемляющие человеческое достоинство, являются «бесчеловечными деяниями» в соответствии с Римским Статутом[24]. Таким образом, Трибунал расширяет толкование этого термина, выходя за рамки Статута и охватывая новые преступные деяния. Такое мнение Трибунала является результатом доктринального вакуума в отношении определения «бесчеловечных деяний». Кроме того, МТБЮ устанавливает элементы, по которым деяние может быть признано бесчеловечным:

– тяжесть совершенных деяний;
– психологический или физический вред или ущерб человеческому достоинству;
– субъективная сторона[25].

В деле Prosecutor v Milorad Krnojelac[26] бесчеловечные деяния также определяются как преднамеренные действия, наносящие серьезный психологический или физический ущерб невиновным лицам[27]. Эта императивная норма квалифицирует действия преступников как преступления против человечности в силу тяжести их последствий. Европейский суд по правам человека в делах Liu v Poland[28] и M. T. and Others v. Sweden[29] использует термин «бесчеловечный» для обозначения действий, унижающих достоинство человека и нарушающих его основные права.

Таким образом, международная судебная практика устанавливает, что эти действия относятся к категории ППЧ, а именно к категории «другие бесчеловечные деяния». Данный термин принят в качестве условия в целях расширения юрисдикции в отношении преследования преступлений против человечности для обеспечения эффективной защиты. Таким образом, Римский статут отражает гибкую судебную практику, позволяющую использовать расширенную юридическую терминологию для контекстуализации не включенных в него злодеяний.

2.3. Применимость категории «другие бесчеловечные деяния» к кибертерроризму

В литературе, посвященной контекстуальным элементам термина «другие бесчеловечные деяния», подчеркивается их тяжесть; эксперты исходят из того, что такие деяния наносят ущерб психологическому и физическому благополучию невинных людей. Анализ этих элементов отражает крайнюю тяжесть этих деяний. Таким

---

24 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522.

25 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

26 IT-97-25-T.

27 Там же, прим. 382.

28 Application no. 37610/18, on 6 October 2022.

29 Application no. 22105/18, on 20 October 2022.

образом, другие действия, выражающие такие же злодеяния, должны быть также классифицированы как «другие бесчеловечные деяния», если в них присутствуют те же контекстуальные элементы. Иначе говоря, определяющим фактором такой классификации деяния является применимость к нему этих элементов.

Прежде всего, кибертерроризм нарушает основные принципы международного гуманитарного права (Werle & Jeßberger, 2014). Во-первых, он нарушает минимальные стандарты человечности, распространяя угрозы. Во-вторых, причиняемый им ущерб гражданскому населению выходит за рамки стандартов соразмерности, поскольку преступный умысел террористов относится ко всем людям. Кибертеррористы ставят во главу угла достижение своих целей, невзирая на страдания невинных гражданских лиц. Этот недискриминационный характер кибертерроризма согласуется с интерпретацией преступлений против человечности Римским статутом[30]. Согласно Статуту, для признания преступления принадлежащим этой категории необходимо, чтобы деяние было совершено против гражданского населения. В международном праве общепризнано, что ущерб от этих преступлений может являться как физическим, так и психологическим. Даже простое пренебрежение человеческим достоинством значительно усугубляет выдвинутые обвинения[31].

В работе С. Маргарити жертвой кибертерроризма выступает все международное сообщество, поскольку он направлен против всеобщего мира и безопасности (Margariti, 2017). Кроме того, общим для кибертерроризма и преступлений против человечности является систематический характер преступлений против человечности, на который указывает Гоббс (Hobbs, 2017). Также оба этих вида преступлений имеют транснациональные последствия, что дает основания для международного вмешательства. Они представляют собой угрозу человечеству, что позволяет отнести их к одной категории. Кроме того, как указывает Р. Атаджанов, элемент систематичности применим к кибертерроризму, поскольку он угрожает всеобщему миру и безопасности и представляет собой широкомасштабное организованное нападение на гражданское население (Atadjanov, 2019). Кибертерроризм причиняет серьезный вред международному сообществу, поскольку его участники ставят под угрозу основные права человека. Их систематические действия нарушают «мирное сосуществование» (Atadjanov, 2019) целевых групп и принципы человечности, предусмотренные Всеобщей декларацией прав человека 1948 г.[32] Кроме того, к кибертерроризму применим такой контекстуальный элемент, как систематический характер ППЧ, поскольку он угрожает всеобщему миру и безопасности и представляет собой широкомасштабное недискриминационное организованное нападение на гражданское население.

Данное мнение подтверждает и обсуждаемое в литературе утверждение о том, что кибертерроризм, причиняющий нефизический ущерб, является преступлением против человечности. Такие деяния направлены на гражданское население в целом, без каких-либо различий, и преступники намеренно игнорируют жертвы среди гражданского населения при достижении своих целей. Более того, Комиссия по международному праву в проекте Конвенции о предупреждении и наказании преступлений

30 The Rome Statute, Art 7.

31 Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494.

32 The Universal Declaration of Human Rights, the United Nations, GA-Res 217/1948. https://clck.ru/36ktDK

против человечности считает психологический ущерб достаточным для квалификации деяния в качестве преступления против человечности[33]. Таким образом, в доктрине международного права физический ущерб не является основным условием совершения преступлений против человечности. Аналогичным образом, международная судебная практика устанавливает, что душевные страдания достаточны для квалификации действий преступников в качестве преступлений против человечности в соответствии со ст. 7 (1) (k) Статута. Такой подход подчеркивает серьезность психологического ущерба, наносимого кибертерроризмом.

При этом ряд ученых не требует наличия оговорки о недискриминационном характере деяния для квалификации его в качестве преступления против человечности (Maguir, 2022). Так, Р. Магуайр утверждает, что они должны носить систематический характер в отношении групп гражданского населения с осознанием преднамеренности действий исполнителей. Аналогичным образом Апелляционной палатой Специального трибунала ООН по Ливану было указано, что субъективной стороной таких деяний должно быть намерение распространить террор с помощью средств, представляющих опасность для гражданского населения[34]. Также было отмечено, что обычное международное право не ограничивает терроризм определенными средствами. Таким образом, признается, что террористы могут использовать кибернетические средства для достижения своих целей. Определяющим фактором является намерение осуществить публичный террор, независимо от формы преступного поведения.

Кроме того, Цилонис отмечает, что понятие «организационная политика», предусмотренное ст. 7 (2)(a) Римского статута, распространяется и на негосударственных субъектов, например, террористов (Tsilonis, 2019). Террористическая деятельность может не поддерживаться государством, чтобы МУС имел право преследовать ее исполнителей. Цель этого положения – усилить защиту человечества от тяжких преступлений. Правовые цели ст. 7 выходят за рамки буквального толкования указанного термина и подразумевают террористическое поведение.

Указанные элементы бесчеловечных деяний совпадают с определением кибертерроризма, которое предлагает В. Коррейя (Correia, 2022). Как в практике, так и в доктрине международного права установлено, что преднамеренные тяжкие деяния, направленные против невиновных гражданских лиц и наносящие ущерб их основным правам, являются, независимо от их формы, бесчеловечными деяниями в соответствии со ст. 7 Римского статута. Очевидно, что это определение можно применить и к кибертерроризму. Нанося удары по инфраструктуре страны, кибертеррористы затрагивают гражданское население. Кроме того, широкомасштабные атаки необходимы преступникам для устрашения общества, что является отличительной чертой их деятельности. Далее, кибертеррористы всегда действуют против всего гражданского населения, а не отдельных его групп. Наконец, для достижения своих целей преступники должны терроризировать невинных людей. Анализ элементов киберпреступлений, приведенный в работе А. Перлофф-Джайлс (Perloff-Giles, 2018), согласуется с содержанием императивных норм, установленных международными судами. Сюда относятся, в частности, примеры бесчеловечных

33 The International Law Commission, “Report of the International Law Commission”, Seventy-first session (29 April – 7 June and 8 July – 9 August 2019) A/74/10, с. 12. https://clck.ru/36ktFT

34 The UN Special Tribunal of Lebanon Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, 16 February 2011, Case No. STL-11-01/1 (STL Decision).

деяний в нарушение прав человека, приведенные в Европейской конвенции по правам человека. Действительно, кибертерроризм изобилует примерами деяний, унижающих человеческое достоинство.

В заключение следует отметить, что ученые и юристы-практики развивают доктрину кибертерроризма как преступления против человечности в соответствии с Римским статутом. Кибертеррористы систематически находят новых жертв, не считаясь с серьезными последствиями. Транснациональный характер таких преступлений дает основания для борьбы с ними на международном уровне. Независимо от используемых методов, состояние страха, которое навязывают преступники, уже само по себе является достаточным основанием для того, чтобы считать кибертерроризм преступлением против человечности. Кроме того, распространение юрисдикции Международного уголовного суда на преследование кибертеррористов позволяет квалифицировать их действия как преступления против человечности. Категория бесчеловечных деяний, предусмотренная ст. 7 (1) (k) Римского статута, должна включать в себя кибертерроризм. Этот вывод предполагает использование универсальных правовых механизмов, находящихся под юрисдикцией МУС, для преследования кибертеррористов. Таким образом, кибертеррористы попадут под юрисдикцию МУС, как и в случае с другими лицами, совершившими преступления против человечности.

3. Универсальная юрисдикция для преследования ППЧ

Развитие международного сотрудничества в судебной сфере привело к возникновению универсального принципа юрисдикции. Этот принцип предполагает возможность преследовать и судить преступников независимо от их местонахождения или гражданства. Он направлен на достижение правосудия на международном уровне, требуя выхода за рамки традиционных юрисдикций для пресечения тяжких преступлений. В работе Блешич (Blešić, 2022) применение универсальной юрисдикции ограничено международными преступлениями, поскольку они налагают всеобщее обязательство преследовать виновных.

Концепция универсальной юрисдикции представляет собой значительное достижение в международном уголовном праве, поскольку она позволяет государствам и соответствующим органам осуществлять преследование международных преступников на глобальном уровне, независимо от их гражданства (Mung'omba, 2022). Таким образом, универсальная юрисдикция ограничивает их возможности избежать наказания, способствуя укреплению международного уголовного правосудия. Она представляет собой право международного сообщества вмешиваться везде, где совершены ППЧ, с целью наказать преступников (Mung'omba, 2022). Примечательно, что, по мнению исследователя, универсальная юрисдикция не требует прямой связи между судебным органом, осуществляющим преследование, и преступлением (Mung'omba, 2022). Универсальная юрисдикция, по его мнению, отличается от основных норм в этой области, что соответствует ее предназначению в обеспечении международного уголовного правосудия (Mung'omba, 2022)[35]. Это отличие обусловлено необходимостью обеспечить

[35] При этом было вынесено решение, что преступник должен лично присутствовать в суде согласно принципам Принстона. См. также Global Policy Forum. (2021, June 2). Princeton Principles on Universal Jurisdiction: Princeton Project on Universal Jurisdiction. https://clck.ru/36ktLY

правосудие и сдерживание в отношении ППЧ (Mung'omba, 2022). Таким образом, универсальная юрисдикция оформлена в международном праве как уникальное средство преследования и сдерживания преступлений против человечности. На уровне ООН делегации государств на 73-й юридической сессии приняли решение, что универсальная юрисдикция представляет собой эффективный инструментарий для преследования основных видов преступлений, в том числе и ППЧ[36].

Можно утверждать, что государства устанавливают национальную юрисдикцию как на субъективной, так и на объективной основе (Kittichaisaree, 2017). Международная судебная практика ограничивает национальную юрисдикцию традиционными факторами[37], тем более что не существует конвенции, устанавливающей нормы универсальной юрисдикции. Более того, суды различных стран должны применять свою «презумптивную юрисдикцию» в отношении преступлений против человечности. Как утверждает Магуайр, интересы жертв оправдывают приоритет национального преследования за эти преступления (Maguir, 2022). Однако другие исследователи критикуют такой подход, считая, что он приведет к злоупотреблению властью со стороны отдельных государств и лишит обвиняемого права на справедливое судебное разбирательство (Soler, 2019). Таким образом, применение универсальной юрисдикции в отношении ППЧ должно быть справедливым и пропорциональным, чтобы гарантировать эффективное правосудие (Soler, 2019). Эти условия поддерживают баланс между противодействием преступлениям против человечности и уважением национального суверенитета. Также этот ученый призывает выработать единый подход к отказам от принципа aut dedare aut judicare, чтобы покончить с безнаказанностью лиц, совершивших ППЧ, которая считается основной причиной того, что такие преступления продолжаются (Maguir, 2022). Таким образом, надлежащее применение универсальной юрисдикции способствует укреплению международного уголовного правосудия, поскольку расширяет юрисдикционные инструменты для преследования и экстрадиции лиц, совершивших ППЧ. Кроме того, такое применение способствует выполнению государствами своих обязательств по преследованию основных преступлений, тем самым они защищают права человека и укрепляют традиционное понимание принципов правопорядка (Maguir, 2022). Примечательно, что Солер отстаивает право третьих государств на преследование лиц, совершивших преступления против человечности, утверждая, что универсальная юрисдикция восполняет отсутствие территориальной юрисдикции и юрисдикции на основе гражданства (Maguir, 2022). Универсальная юрисдикция, таким образом, не противоречит обязанности государства преследовать указанные преступления (Maguir, 2022).

Хотя принцип универсальной юрисдикции ограничивает безнаказанность преступников, она может рассматриваться и как угроза национальному суверенитету и стабильности[38]. Так, Африканский союз отклонил испанский ордер на арест генерал-лейтенанта Эммануэля Каренци Караке, посчитав его нарушением международного права и злоупотреблением принципом универсальной юрисдикции. Союз также осудил попытки

---

36 The 6th Committee of the UN General Assembly – Legal (73rd Session), 'The scope and application of the principle of universal jurisdiction (Agenda item 87)', См. resolution 72/120. https://clck.ru/36ktQV

37 См. the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

38 African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

европейских судов подчинить себе судебные органы африканских стран путем злоупотребления универсальной юрисдикцией[39]. Эти факты отражают противоречивость принципа универсальной юрисдикции. Данный механизм позволяет преследовать за преступления против человечности и положить конец безнаказанности преступников, их совершающих, однако его применение не лишено недостатков. В работе Ньяво это обосновывается отсутствием международного соглашения или иного документа, определяющего универсальную юрисдикцию и объясняющего ее применение (Nyawo, 2023). Ученый утверждает, что универсальная юрисдикция необходима для противодействия ППЧ, поскольку в этом заинтересованы все государства (Nyawo, 2023). Кроме того, он обосновывает необходимость использования универсальной юрисдикции всеобщим моральным долгом, который постулируется в теории естественных прав (Nyawo, 2023). Этот долг обязывает международное сообщество сотрудничать в борьбе со злодеяниями, угрожающими миру и безопасности на планете.

Совет безопасности ООН также говорит об обязанности преследовать преступления против человечности и наказывать виновных, независимо от их гражданства[40]. Данная резолюция отражает понимание ППЧ как особо тяжких преступлений, подразумевая единую модель преследования виновных.

Представитель организации Human Rights Watch Лотте Лейхт утверждает, что ООН разработала механизм судебного преследования лиц, совершивших ППЧ. Этот механизм предусматривает работу постоянного прокурора, который инициирует расследование случаев преступлений против человечности, не создавая специального суда. Его юрисдикция распространяется повсеместно, независимо от судебных или политических барьеров[41].

3.1. Принцип aut dedere aut judicare в отношении кибертерроризма

Аксиомой международного права является положение о том, что обвинения в терроризме предполагают применение универсальной юрисдикции в силу их тяжести (Soler, 2019). Поскольку принцип aut dedare aut judicare представляет собой общий принцип международного права, международное сообщество должно использовать его для борьбы с кибертерроризмом. Тяжесть этого преступления, недостаточность защиты прав человека на международном уровне, а также угроза миру вследствие безнаказанности кибертеррористов – все это свидетельствует в пользу применения универсальной юрисдикции как международными, так и национальными судами с целью преследования и выдачи преступников. Только таким образом может быть обеспечено сдерживание кибертерроризма на глобальном уровне.

Характеризуя киберпреступников как врагов человечества, А. Перлофф-Джайлс (Perloff-Giles, 2018) поддерживает введение универсальной юрисдикции для преследования и выдачи кибертеррористов. Она также утверждает, что в соответствии с Конвенцией ООН по морскому праву (UNCLOS) государства могут преследовать пиратов, где бы они ни действовали, в том числе «вне территориальных вод», т. е. вне

39 Там же, para 6.

40 UNSC/S/RES/138, 23 June 1960, para 4. https://clck.ru/36ktdL

41 The European Parliament. (2018, June 28). Workshop: Universal jurisdiction and international crimes: Constraints and best practices. Brussels, EP/EXPO/B/COMMITTEE/FWC/2013-08/Lot8/21.

пределов национальной юрисдикции[42]. Затем исследователь расширяет понятие «вне территориальных вод», включая в него киберпространство, поскольку считает его транснациональной сферой взаимодействия (Perloff-Giles, 2018). Свою точку зрения она обосновывает решением американского суда, постановившего, что нахождение «вне территориальных вод» не является условием для применения универсальной юрисдикции в отношении пиратства[43]. Сравнивая пиратство и киберпреступность, ученый показывает, что и то и другое угрожает международной торговле, поскольку кибератаки могут нарушить работу сайтов коммерческих и финансовых служб. Таким образом, принцип универсальной юрисдикции является эффективным подходом к пресечению транснациональных киберпреступлений.

Применение принципа универсальной юрисдикции осложняют технические вопросы, например, облачные вычисления, поскольку в киберпространстве сразу несколько государств могут заявить о своей экстерриториальной юрисдикции в отношении облачной деятельности, как было показано в работе (Kittichaisaree, 2017). Рассматривая международно-правовые документы, ученый упоминает, что разрешение на экстерриториальное преследование «несанкционированной трансляции сигнала» с судна, находящегося вне территориальных вод[44], распространяется и на передачу сигналов кибернетическими средствами (Kittichaisaree, 2017). Таким образом, он применяет термин «вещание» к интернет-сайтам, таким как Facebook[45] и Twitter[46]. Эти онлайн-платформы используются террористами для трансляции своей идеологии и вербовки, что дает основания государствам применять свою юрисдикцию. Кроме того, Конвенция 1973 г. о предотвращении и наказании за преступления против лиц, пользующихся международной защитой, устанавливает универсальную юрисдикцию в отношении преступных деяний, которая распространяется и на кибертерроризм, если они направлены против лиц, указанных в ст. 1[47]. Это требует от государств-участников использовать свои правовые инструменты для пресечения этой деятельности, в соответствии с целями Конвенции. В связи с быстрым развитием средств доступа в Интернет затраты на организацию кибертеррористической деятельности очень малы по сравнению с ее последствиями (Kittichaisaree, 2017). Поэтому необходимо расширить область применения Будапештской конвенции о киберпреступности и создать глобальную сеть для преследования кибертеррористов.

Как утверждает Магуайр, преследование кибертерроризма в рамках национальных судебных систем оказывается эффективным, поскольку оно мотивировано доверием пострадавших к этим системам[48]. Кроме того, презумптивная юрисдикция отражает в своей основе применение к этим преступлениям универсальной юрисдикции;

---

42 Article 101 c of the United Nations Convention on the Law of the Sea, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994).

43 United States v. Ali, 718 F.3d 929, 935-38 (D.C. Cir. 2013).

44 Art 109, the UNCLOS.

45 Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

46 Социальная сеть заблокирована на территории Российской Федерации за распространение незаконной информации.

47 Art 3 of the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, entered into force on 20 February 1977.

48 См. the Lotus Case (France v. Turkey), Judgment of 7 Sept. 1927, Series A No. 10.

тем самым обеспечивается защита пострадавших от юрисдикционной уязвимости, связанной с преследованием кибертерроризма (Kittichaisaree, 2017). Следовательно, такой подход соответствует принципу экстерриториального наказания киберпреступников, независимо от их местонахождения или гражданства. При этом последствия кибертерроризма могут затрагивать несколько юрисдикций, что приводит к их конфликту. Таким образом, принцип взаимодополняемости МУС сохраняет свое значение для устранения недостатков государственных органов в преследовании кибертеррористов. Однако эта система обратной комплементарности отражает вертикальную иерархию между Международным уголовным судом и его членами в вопросе преследования основных преступлений (Burens, 2016). Так, Лаура Буренс утверждает, что горизонтальный межгосударственный механизм взаимодополняемости усиливает принцип универсальной юрисдикции в соответствии с Римским статутом. Кроме того, ее подход включает государство, в котором находится преступник, в качестве обязательного условия для использования универсальной юрисдикции в процессе уголовного преследования (Burens, 2016). Такая интеграция вертикальной и горизонтальной взаимодополняемости устраняет проблемы применения универсальной юрисдикции благодаря прозрачности принципа субсидиарности (Burens, 2016)[49]. Кроме того, в Резолюции 72/120 отмечается, что использование принципа универсальной юрисдикции должно подчиняться действию международного права и принципу субсидиарности, чтобы предотвратить злоупотребления или неэффективное использование данного принципа[50]. Солер, в свою очередь, утверждает, что такая интеграция необходима для адекватного применения универсальной юрисдикции, чтобы преодолеть недостаточность принципа субсидиарности (Soler, 2019).

Что касается национальных законов, то законодательство Великобритании распространяет свою юрисдикцию на террористические преступления, независимо от их объективной стороны, в соответствии с целями, указанными в ст. 63B[51]. Такая экстерриториальная юрисдикция способствует защите от кибертерроризма: Королевская уголовная прокуратура может использовать свои правовые инструменты для экстерриториального преследования преступников[52], если указанная статья содержит указания на их субъективную сторону. Кроме того, судебные органы Великобритании в деле R v. Kumar Lama[53] указали, что национальный суд должен использовать универсальную юрисдикцию для преследования тяжких преступлений. При этом стоит отметить, что данный процесс подвергался критике из-за недостатков сбора доказательств за рубежом, которые привели к тому, что суд признал полковника Ламу невиновным[54]. Аналогичным образом Закон о борьбе с преступлениями в сфере информационных

---

49 Л. Буранс утверждает, что данный принцип служит поддержанию баланса между суверенитетом государств и необходимостью преследовать международных преступников.

50 Resolution 72/120, Supra 17.

51 Terrorism Act 2000, the UK, 63A- 63D.

52 The Crown Prosecution Service (2021), 'Jurisdiction', (CPS: Legal Guidance on 26 July 2021). https://clck.ru/36ktjD

53 Case no. 2013/05698 (Central Criminal Court, London, 2016).

54 Hovell, D. (2017, April 6). The 'Mistrial' of Kumar Lama: Problematizing Universal Jurisdiction. EJIL Talk – Blog of the European Journal of International Law. https://clck.ru/36ktkR

технологий[55] расширил юрисдикцию Египта в отношении киберпреступлений, включив в нее преступления, совершенные неграждanами при следующих условиях[56]:

– Преступление было совершено на борту любого морского, воздушного или наземного транспорта, зарегистрированного в Египте или функционирующего под его флагом.

– Жертвой является гражданин Египта.

– Преступление планировалось, отслеживалось или финансировалось в Египте.

– Преступление совершено организованной группой, действовавшей в нескольких странах, в том числе и в Египте.

– Преступление может нанести ущерб интересам или безопасности Египта, а также интересам или безопасности любого гражданина или жителя страны.

– Преступник был обнаружен в Египте после совершения преступления и еще не был экстрадирован.

Такой широкий подход египетского законодателя является следствием правового вакуума, в котором оказались египетские судьи в отношении кибертерроризма. Он также демонстрирует комплексный взгляд на применение универсальной юрисдикции в киберпространстве для усиления правовой защиты от кибертерроризма.

В заключение следует отметить, что транснациональный характер кибертерроризма, а также его серьезное влияние на всеобщий мир и безопасность подталкивают международное сообщество к принятию универсальной юрисдикции для преследования и наказания виновных. Этот подход является адекватным механизмом для противостояния киберпреступникам, поскольку согласуется с обязанностями государства по преследованию основных преступлений, признанными в международном праве. Действительно, безнаказанность кибертеррористов ведет к росту числа их преступлений. Поэтому международное сообщество должно объединить свои правовые усилия для выработки единого глобального понимания принципа универсальной юрисдикции, чтобы избежать правового вакуума.

4. Заполнение пробела в законодательстве

Общепризнано, что кибертерроризм является одним из основных видов противоправной деятельности в киберпространстве в силу возможностей последнего. Широкий охват, распространяющийся и на реальный мир, позволяет преступникам эффективно достигать своих целей. Таким образом, складывается глобальная тема кибертерроризма, для противостояния которому необходимо использовать международно-правовые механизмы. Однако глобальный характер этих механизмов может превратить их в инструменты вмешательства во внутренние дела независимых государств. Проще говоря, государства могут выступать против использования этих механизмов, обосновывая это соображениями суверенитета. Возникает дилемма в отношении преследования и суда над кибертеррористами, что усиливает их безнаказанность в реальной международно-правовой практике. Таким образом, они угрожают миру и безопасности на планете. Чтобы преодолеть противодействие государств и убедить их в необходимости сотрудничества в борьбе с кибертерроризмом как

[55] Law No 175/2018.

[56] Там же, pt 1 art 3.

международной опасностью, эти глобальные механизмы должны иметь прочную правовую основу.

4.1. Объяснение существующей дилеммы

Несмотря на стабильность международно-правовых норм, их применение еще не стало чем-то само собой разумеющимся. Различные интересы государств и интерпретация ими международно-правовых концепций затрудняют создание единого порядка применения международных императивных норм. Возвращаясь к теме исследования, международно-правовая практика показывает, что обе нормы международного права – принципы R2P и универсальной юрисдикции – постоянно подвергаются сомнению. Скептиками выступают либо юристы, либо дипломаты, поскольку отсутствует единство в понимании этих концепций. Таким образом, попытка закрепить принцип универсальной юрисдикции на основе концепции R2P принесет результат только в том случае, если позиция ее критиков также будет тщательно изучена, а ее траектория контекстуализирована.

Международно-правовая практика показывает, что применение универсальной юрисдикции для противодействия кибертерроризму еще не стало приемлемым механизмом. Многие государства и даже международные организации выступают против него и препятствуют осуществлению правовых мер, основанных на принципе универсальной юрисдикции. Такое противодействие, очевидно, проявилось и в заявлении Африканского союза, где говорилось, что универсальная юрисдикция нарушает стабильность всего континента[57]. Хотя принятые европейским судом меры касались ППЧ в Руанде, они были восприняты в чисто политическом контексте, связанном с воспоминаниями о европейской колонизации Африки. Подобные взгляды усиливают безнаказанность преступников и препятствуют осуществлению правосудия.

Кроме того, дискуссии на 12-м заседании Шестого комитета Генеральной Ассамблеи ООН обнаружили существенный пробел в отношении универсальной юрисдикции. В то время как Германия представила опыт судебного преследования официальных лиц Сирии в национальном суде за совершение преступлений против человечности[58], Колумбия заявила, что применение универсальной юрисдикции должно осуществляться на основании двустороннего или международного договора[59]. Большинство представителей отметили, что для эффективности универсальной юрисдикции необходимо ее включение в национальные правовые системы[60]. Тем самым прослеживается различие в отношении государств к универсальной юрисдикции, что углубляет разрыв в ее концептуализации и применении. Кроме того, государства могут выступать против универсальной юрисдикции, поскольку не желают разрешать иностранной юрисдикции преследовать кибертеррориста на своей территории и выдавать его иностранной юрисдикции. Так, Блешич утверждает,

---

57 African Union Doc PSC.PR/COMM.(DXIX) Communiqué, Peace and Security Council 519th, 26 June 2015, paras 4-5. https://clck.ru/36ktSW

58 Speakers Disagree on How, When, Where Universal Jurisdiction Should Be Engaged, as Sixth Committee Takes up Report on Principle. (2022, October 12). UN Press. https://clck.ru/36ktp8

59 Там же, para 7.

60 Там же, paras 3, 4, 5 & 8.

что определяющим фактором применения универсальной юрисдикции является политическая воля (Blešić, 2022). Она, в свою очередь, зависит от наличия двусторонних договоров между государствами.

Более того, децентрализация международного уголовного правосудия приводит к тому, что универсальная юрисдикция зависит только от воли и действий государств (Nyawo, 2023). Это существенный недостаток, поскольку может привести к политическим конфликтам между государствами, особенно в условиях отсутствия всеобщих правил в отношении универсальной юрисдикции. Разработка международно-правовых норм является необходимым условием стабилизации судебного статуса в отношении уголовного преследования за совершение преступлений против человечности. Таким образом, для преодоления этого барьера универсальная юрисдикция нуждается в универсальном обосновании, соответствующем ее целям и природе.

В международной доктрине отмечается, что концепция R2P имеет ряд недостатков. По словам Ройер, практика международного права показывает, что государства могут рассматривать принцип R2P как отражение западного империализма (Royer, 2021). Он утверждает, что этому мнению способствует использование данной концепции для оправдания военных интервенций в случае совершения ППЧ (Royer, 2021). Кроме того, концепция R2P угрожает равновесию при поддержании правопорядка (Royer, 2021), что приводит к хаосу внутри государства. Эта дихотомия лежит в основе критики R2P (Royer, 2021). Поэтому ученый предлагает юристам обратить особое внимание на этот аспект данной концепции, чтобы гарантировать беспристрастность его применения (Royer, 2021). Далее он утверждает, что доктрина должна оценивать вмешательство в рамках концепции R2P отдельно по каждому случаю (Royer, 2021), чтобы избежать несправедливости в международно-правовой практике (Royer, 2021). Обобщение суждений о R2P ставит под угрозу доверие к этой гуманитарной концепции, а злоупотребление ею ни в коем случае не должно приводить к отказу от нее. Поэтому определяющим фактором применения R2P являются обстоятельства каждого конкретного дела. Такой механизм отделяет этот принцип от политической воли государств и способствует его беспристрастному применению. Наконец, по мнению Ройер, критиковать концепцию R2P могут лишь те, кто неспособен оценить последствия зла, которому она противостоит.

Таким образом, необходимость применения принципа универсальной юрисдикции против кибертерроризма перевешивает доводы, объясняющие противодействие государств. Кибертерроризм как глобальное преступное деяние требует использования международного инструментария, выходящего за рамки внутренних правовых границ и преследующего кибертеррористов независимо от их местонахождения. Теория R2P является адекватным основанием для введения универсальной юрисдикции в отношении кибертерроризма.

4.2. Решение: применимость концепции R2P для введения универсальной юрисдикции в отношении кибертерроризма

В правовой доктрине кибертерроризм рассматривается как международное зло (Margariti, 2017), поскольку его последствия для всеобщего мира и безопасности соответствуют таковым у ППЧ. Международное сообщество страдает от обоих видов преступлений (Margariti, 2017), однако кибернетическая составляющая отличает

кибертерроризм как современное зло (Perloff-Giles, 2018). Это эволюционировавшая разновидность преступлений против человечности, которая относится к категории «другие бесчеловечные деяния». Это очевидно, исходя из совпадения элементов кибертерроризма с контекстуальными элементами ППЧ, как показывает судебная практика[61]. Следовательно, универсальная юрисдикция необходима как глобальный механизм преследования и экстрадиции террористов. Однако противодействие применению универсальной юрисдикции[62] требует наличия твердых оснований для ее применения. Такой опорой является теория R2P.

В представленном обзоре отмечается значимость теории R2P в международном праве. Данная концепция была разработана как инструмент защиты человечества. Основной целью R2P является защита человечества от злодеяний. Таким образом, ее применение для противостояния ППЧ доказывает ее значимость в международной доктрине и правовой практике. R2P, как считает Ройер, является гуманитарным инструментом предотвращения зла, поскольку оправдывает юридическое вмешательство для преследования виновных в ППЧ (Royer, 2021). При этом во главу угла ставится защита отдельных людей, а не сохранение суверенитета в Вестфальском понимании[63].

Ройер высоко оценивает гибкость механизма R2P, поскольку он позволяет достичь баланса с гуманитарными потребностями в предотвращении преступлений против человечности (Royer, 2021). Ученый переосмысливает R2P с позиции морали, поскольку это механизм противостояния злу (Royer, 2021). Как следствие, политическая воля не может противостоять нормам, которые на ней же и основаны. Напротив, концепция R2P объединяет политические интересы государств и мораль человечества в единый инструмент, направленный против злодеяний (Royer, 2021). Фактически это инструмент как политики, так и морали, который защищает людей от злодеяний (Royer, 2021). Такое переосмысление R2P доказывает правомерность использования норм международного права для пресечения ППЧ. Примечательно, что в своем видении R2P Ройер гармонично сочетает его с требованием государственного суверенитета, который в своей основе также является защитой от злодеяний, поскольку организует автономное управление внутренними делами государства. Следовательно, он борется с беспорядком внутри страны, которым могут воспользоваться злоумышленники для достижения своих целей (Royer, 2021). Таким образом, суверенитет отражает обязанность государства защищать граждан.

Как показывает практика МУС, коллективные обязательства государств побуждают их к принятию универсальных инструментов для искоренения ППЧ с целью обеспечения мира во всем мире[64]. Природа универсальной юрисдикции не противоречит этой цели; преследование преступлений против человечности на международном уровне ограничивает их распространение и укрепляет правосудие. Поскольку концепция R2P допускает военное вмешательство для борьбы с ППЧ, она также оправдывает и судебное вмешательство, т. е. введение универсальной юрисдикции.

---

61 Prosecutor v Muci´c et al, Trial judgment, 16 November 1998, IT-96-21-T, (Celebici˘, Trial judgment), paras 521–522; Prosecutor v Karadži´c, Trial judgment, 24 March 2016, IT-95-5/18-T, (Karadži´c, Trial judgment), para 494; IT-97-25-T.

62 См. обсуждение в предыдущем разделе.

63 Resolutions 1674 (2006), 63/308 (2009)68 and 1894 (2009).

64 Application of the Convention on the Prevention and Punishment of the Crime of Genocide (BiH v Serbia and Montenegro), 26 February 2007, ICJ Reports 2007 p. 43, para 166.

Поскольку, как показано в исследовании, кибертерроризм является преступлением против человечности, то концепция R2P должна оправдывать преследование кибертеррористов на международном уровне. Из этого следует, что суд или отдельный прокурор может преследовать кибертеррориста, находящегося на территории другой юрисдикции, если территориальная юрисдикция не проявляет к нему должного внимания. В этом случае, согласно объяснению Лауры Буренс (Burens, 2016), действует принцип горизонтальной взаимодополняемости. Концепция R2P оправдывает такое судебное вмешательство, поскольку международное сообщество обязано предотвращать ППЧ, как это установлено международным обычным правом. Судебное вмешательство для противодействия преступлениям против человечности лучше военного, поскольку оно повышает доверие к международному уголовному правосудию и устраняет угрозу человечеству со стороны кибертеррористов.

Заключение

Исследование посвящено изучению концепции R2P, анализу ее компонентов и комплексного представления о ней в международном праве. Данная концепция представляет собой превентивный инструмент для защиты человечества от злодеяний. О его значении можно судить по тому, что его применение было неоднократно санкционировано СБ ООН и международным сообществом для вмешательства в пресечение ППЧ. Это общий принцип международного права. Кроме того, юридический анализ доказывает гибкость механизма R2P, поскольку он применяется различным образом в каждом конкретном случае. Концепция R2P используется для обоснования военных операций и юридического вмешательства для преследования ППЧ. Изученные факты доказывают пригодность R2P для выполнения данной задачи.

Также в исследовании анализируется кибертерроризм. Это современная преступная деятельность, наносящая ущерб государствам. В доктрине он рассматривается как общий враг человечества, поскольку угрожает миру и безопасности во всем мире. Анализируя элементы этого явления, мы сопоставляем их с контекстуальными элементами ППЧ и делаем вывод об их конгруэнтности. Это означает, что кибертерроризм является преступлением против человечности согласно Римскому статуту. Категория «другие бесчеловечные деяния» распространяется и на кибертерроризм. Следовательно, международное сообщество должно принять меры по преследованию и наказанию кибертеррористов, чтобы устранить их безнаказанность.

Внешнее судебное вмешательство осуществляется в международном частном праве посредством универсальной юрисдикции. Она включает в себя использование национальных судебных инструментов в рамках других юрисдикций, поэтому сталкивается с рядом препятствий со стороны государств и даже региональных организаций. Эти препятствия сводят на нет международно-правовые усилия по пресечению кибертерроризма. Таким образом, необходимо найти адекватное юридическое обоснование универсальной юрисдикции, которое открыло бы международному сообществу путь к преследованию кибертеррористов.

Далее в работе представлен принцип R2P как необходимое обоснование универсальной юрисдикции в отношении кибертерроризма. Поскольку кибертерроризм представляет собой угрозу миру и безопасности во всем мире, международное сообщество должно принять меры по его искоренению с помощью механизмов универсальной юрисдикции. Такое вмешательство соответствует нормам международного права, так как обеспечивает защиту прав человека, что является его главной целью.

Наконец, представленное исследование устраняет разрыв между нормами международного публичного права и международного частного права, применяя теорию R2P из первого для обоснования универсальной юрисдикции из второго. Такое сочетание демонстрирует взаимодополняемость отраслей международного права, что служит глубокому пониманию международных киберпроблем.

Список литературы

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Сведения об авторе

Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре
Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Конфликт интересов

Автор сообщает 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: 10.77.51 / Отдельные виды преступлений
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 23 июля 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.43

Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism

Yassin Abdalla Abdelkarim

Luxor Elementary Court
Sohag, Egypt

Keywords

crimes against humanity,
cybersecurity,
cyberspace,
cyberterrorism,
digital technologies,
human rights,
international private law,
international public law,
jurisdiction,
law

Abstract

Objective: the development of wireless technologies and digital infrastructure has radically changed the human habitat, giving rise to a new type of space – a cyberspace. The uniqueness and peculiarities of this environment, including anonymity, boundlessness and problems related to the determination and establishment of jurisdiction, have become a breeding ground for the emergence of a new global threat – cyberterrorism. The latter is characterized by a high level of latency, low detection rate and incomparably greater danger than "real world" crimes. Countering new forms of crime has required the development of universal tools that overcome the limitations of traditional jurisdiction and allow states to prosecute terrorists in cyberspace. Identifying the relevant tools and identifying the political-legal obstacles to their implementation is the objective of this study.

Methods: to achieve the set goal the formal-legal method was used to analyze legal sources, including judicial practice, national legislation, and international acts. The doctrinal approach was also used, which allowed, on the basis of scientific works and theoretical constructions, explaining the complexity of the modern phenomena and predicting their future development. This said, the main focus is on criminals to prove their antagonism with humanity in accordance with theoretical views. Finally, the study analyzes the theories of universal and traditional jurisdiction and how they are applied to prosecute terrorists.

Results: the paper provides a critical analysis, reviewing and adapting the concept of jurisdiction as applied to a global, borderless and decentralized digital environment (cyberspace) and to the struggle against new forms of terrorism (cyberterrorism). Various jurisdictional models applicable in cyberspace are presented. The author bridges the gap between the main branches of law: international private law and public law by linking, in relation to cyberterrorism, the two theories: the "responsibility to protect" (R2P) theory and the application of universal jurisdiction. The trends of universal jurisdiction development are revealed.

Scientific novelty: the study develops the accumulated scientific knowledge while justifying the introduction of foreign jurisdiction in a state territory to prosecute cyberterrorists. It also establishes a link between the theory of universal jurisdiction in private international law and the "responsibility to protect" (R2P) theory in public international law, recognizing the latter as a relevant basis for the introduction of universal jurisdiction over cyberterrorism. Such traditional concepts as sovereignty and jurisdictional independence are reviewed. The gap related to the consideration of cyberterrorism as a crime against humanity in international law is bridged.

Practical significance: the implementation of the proposed conclusions will contribute to the strengthening of international prosecution of cyberterrorism and harmonize the international and national legal tools to struggle against this crime.

For citation

Abdelkarim, Y. A. (2023). Employing the Responsibility to Protect (R2P) to Impose Universal Jurisdiction Regarding Cyber-Terrorism. *Journal of Digital Technologies and Law, 1*(4), 994–1022. https://doi.org/10.21202/jdtl.2023.43

References

Adem, S. H. (2019). Palestine and the International Criminal Court. In Werle, G., & Vormbaum, M. (Eds.), *International Criminal Justice Series*, *21*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-291-0

Albahar, M. (2019). Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. *Science and Engineering Ethics*, *25*(4). https://doi.org/10.1007/s11948-016-9864-0

Atadjanov, R. (2019). Humanness as a Protected Legal Interest of Crimes Against Humanity. Conceptual and Normative Aspect. In G. Werle, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *22*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-299-6

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. *Social Science and Public Policy*, *54*, 138. https://doi.org/10.1007/s12115-017-0114-0

Azubuike, E. C. (2023). Principle of Responsibility to Protect: Implications for Sovereignty. In E. Duruigb, R. Chibueze, & S. G. Ogbodo (Eds.), *International Law and Development in the Global South* (pp. 55–77). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-13741-9_5

Bellamy, A. (2018). Responsibility to Protect: Justice and Responsibility—Related but Not Synonymous. In J. Waterlow & J. Schuhmacher (Eds.), *War Crimes Trials and Investigations* (pp. 263–299). Cham, Switzerland: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-64072-3_9

Blešić, J. (2022). Aut Dedere Aut Judicare in International and Domestic Law. In *Protection of human rights and freedoms in light of international and national standards, Contemporary Problems of the Legal System of Serbia* (pp. 213–224). The Faculty of Law, University of Belgrade.

Broeders, D., Cristiano, F., & Weggemans, D. (2021). Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy, *Studies in Conflict and Terrorism*. https://doi.org/10.1080/1057610x.2021.1928887

Burens, L. (2016). Universal Jurisdiction Meets Complementarity: An Approach towards a Desirable Future Codification of Horizontal Complementarity between the Member States of the International Criminal Court. *Criminal Law Forum*, *27*(1), 75–97. https://doi.org/10.1007/s10609-016-9272-9

Cantini, N., & Zavialov, D. (2018). Fixing Responsibility to Protect: Lessons from and Proposals for the Case of Libya. *Peace Human Rights Governance*, *2*(1), 75. https://doi.org/10.14658/pupj-phrg-2018-1-4

Correia, V. J. (2022). An Explorative Study into the Importance of Defining and Classifying Cyber Terrorism in the United Kingdom, *SN Computer Sciences*, *3*, 84. https://doi.org/10.1007/s42979-021-00962-5

Delerue, F., Desforges, A., & Géry, A. (2019, April 23). A Close Look at France's New Military Cyber Strategy. *War on the Rocks*. https://clck.ru/36ktrj

Ercan, P. G. (2022). *The Responsibility to Protect Twenty Years On: Rhetoric and Implementation*. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-90731-0

Fehl, C. (2015). Probing the Responsibility to Protect's Civilian Dimension: What Can Non-Military Sanctions Achieve? In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 39–57). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1.

Henschke, A. (2021). Terrorism and the Internet of Things: Cyber-Terrorism as an Emergent Threat. In A. Henschke, A. Reed, S. Robbins, & S. Miller (Eds.), *Counter-Terrorism, Ethics and Technology' Advanced Sciences and Technologies for Security Applications*. Springer. https://clck.ru/36ktsa

Hobbs, H. (2017). Towards a Principled Justification for the Mixed Composition of Hybrid International Criminal Tribunals. *Leiden Journal of International Law*, *30*(1), 177. https://doi.org/10.1017/s092215651600056x

Holvoet, M., & Mema, M. (2015). The International Criminal Court and the Responsibility to Protect. In D. Fiott, & J. Koops (Eds.), *The Responsibility to Protect and the Third Pillar: Legitimacy and Operationalization* (pp. 21–38). Palgrave Macmillan, Cham. ISBN 978-1-137-36440-1. https://doi.org/10.1057/9781137364401_3

Kittichaisaree, K. (2017). Future Prospects of Public International Law of Cyberspace. In K. Kittichaisaree, *Public International Law of Cyberspace* (pp. 335–356). Springer. https://clck.ru/36ktuq

MacNeil, G. (2021). Legality Matters: Crimes Against Humanity and the Problems and Promise of the Prohibition on Other Inhumane Acts. In G. W., & M. Vormbaum (Eds.), *International Criminal Justice Series*, 28. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-443-3

Maguir, R. (2022). Prosecuting Crimes Against Humanity: Complementarity, Victims' Rights and Domestic Courts. *Criminal Law and Philosophy*, *17*, 669–689. https://doi.org/10.1007/s11572-022-09648-2

Margariti, S. (2017). Defining International Terrorism: Between State Sovereignty and Cosmopolitanism. In G. Werle, L. Fernandez, & M. Vormbaum (Eds.), *International Criminal Justice Series*, *15* (pp. 1–26). T.M.C. Asser Press, The Hague. ISBN 978-94-6265-204-0. https://clck.ru/36ktwV

Mung'omba, I. (2022). Universal Jurisdiction as a Tool in Promoting Accountability for International Crimes in Africa: Exploring the Significance of Hissene Habre's Conviction. In E. C. Lubaale, & N. Dyani-Mhango (Eds.), *National Accountability for International Crimes in Africa* (pp. 91–114). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-88044-6_4

Nyawo, J. (2023). The Scope and Application of Universal Jurisdiction: A Synopsis of African States' Positions and Proposals During Plenary Sessions in the Sixth Committee of the United Nations General Assembly. In T. B. K. Sendze, A. Adeboyejo, S. Ugwu, & H. Morrison (Eds.), *Contemporary International Criminal Law Issues. Contributions in Pursuit of Accountability for Africa and the World* (pp. 213–262). Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-555-3_7

Park, T. J., & Switzer, M. (2020, May). R2P & Cyberspace: Sovereignty as a Responsibility. In *The 12th International Conference on Cyber Conflict*. Tallin, Estonia. https://doi.org/10.23919/cycon49761.2020.9131729

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(4), 191–227. https://clck.ru/36ktyQ

Quigley, J. (2023). Prohibition of Palestine Arab Return to Israel as a Crime Against Humanity. *Criminal Law Forum*, *38*. https://doi.org/10.1007/s10609-022-09450-8

Royer, Ch. (2021). A Responsibility to Protect Humanity from Evil. In *Evil as a Crime Against Humanity. Ser. International Political Theory* (pp. 81–130). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-53817-0_3

Schmitt, M. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Shandler, R., Gross, M. L., Backhaus, S., & Canetti, D. (2021). Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment, *British Journal of Political Science*. https://doi.org/10.1017/s0007123420000812

Soler, Ch. (2019). *The Global Prosecution of Core Crimes under International Law*. T.M.C. Asser Press, The Hague. https://doi.org/10.1007/978-94-6265-335-1

Stoddart, K. (2022). Non and Sub-State Actors: Cybercrime, Terrorism, and Hackers. In K. Stoddart (Ed.), *Cyberwarfare: Threats to Critical Infrastructure* (pp. 351–399). Springer International Publishing. https://doi.org/10.1007/978-3-030-97299-8_6

Tsilonis, V. (2019). *The Jurisdiction of the International Criminal Court*. Springer Nature Switzerland, Gewerbestrasse, Switzerland. https://doi.org/10.1007/978-3-030-21526-2

Werle, G., & Jeßberger, F. (2014). *Principles of International Criminal Law* (4th ed.). Oxford University Press. ISBN 9780198826859. https://goo.su/Xwzm

Wyatt, S. J. (2019). The Responsibility to Protect and Habermas: Theory of Constitutionalisation with a "Cosmopolitan Purpose". In *The Responsibility to Protect and a Cosmopolitan Approach to Human Protection* (pp. 151–176). New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-00701-0_6

Author information

Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court
Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt
E-mail: yassinabdelkarim91@gmail.com
ORCID ID: https://orcid.org/0000-0001-7388-1337

Conflicts of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt –July 23, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47
EDN: https://elibrary.ru/igaziz
DOI: https://doi.org/10.21202/jdtl.2023.44

Правовая природа смарт-контрактов: договор или программный код?

Гергана Варбанова

Университет национального и мирового хозяйства;
Арбитражный суд BIA
г. Варна, Болгария

Ключевые слова

блокчейн,
гражданское право,
договор,
договорное право,
информационные технологии,
коммерческое право,
право,
программный код,
смарт-контракт,
цифровые технологии

Аннотация

Цель: цифровая экономика и договорные отношения, обусловленные стремительным изменением технологий, определяют трансформацию права и развитие законодательства в направлениях его адаптации к перспективам распространения и применения смарт-контрактов в гражданском и коммерческом обороте, в связи с чем нацеленность исследования на определение юридической сущности смарт-контрактов становится основополагающим этапом на пути к выработке своевременного и четкого их регулирования.

Методы: в основу исследования положена методология формально-юридического и сравнительно-правового анализа, позволяющая сопоставить нормы действующего болгарского законодательства и наднациональных источников права, а также выявить характерные черты смарт-контрактов как востребованных инструментов, необходимых для современного права и экономики, и сопоставить их с классическим пониманием контрактов, в сравнении с которым можно более точно понять и определить природу смарт-контрактов.

Результаты: определено, что смарт-контракт является программным кодом, в котором стороны заранее установили условия, при которых договорные отношения между ними создаются, изменяются и прекращаются; доказано, что исполнение контракта зависит не от действия или бездействия его сторон, а скорее от наступления заранее установленного условия (определенного факта, имеющего отношение к сторонам), при котором контракт должен самоисполняться; обосновано, что воля сторон не может быть изменена или заменена именно из-за особого способа записи смарт-контракта в децентрализованном реестре; выявлено, что основополагающей остается проблема передачи воли с юридического языка в программный код смарт-контракта – если воля сторон неправильно передана в программный код, смарт-контракт может самоисполниться, но его исполнение не будет тем результатом, на который рассчитывали стороны.

Научная новизна: проведенный анализ позволил сравнить современное национальное (болгарское) законодательство и наднациональное (европейское) право, выявив нечеткость регулирования смарт-контрактов как на национальном, так и на международном уровне, определив ряд нуждающихся в научной и правовой интерпретации вопросов о правовой природе смарт-контрактов в контексте концепции самоисполняющегося программного кода.

Практическая значимость: исследование может послужить основой для дальнейшего развития законодательства в направлениях его адаптации к перспективам распространения и применения смарт-контрактов в гражданском и коммерческом обороте, а также для углубленного анализа практики применения смарт-контрактов с точки зрения имеющихся неразрешенных проблем точной передачи воли сторон в программный код (перевода конкретных терминов с юридического языка в программный код смарт-контракта), электронной идентификации субъектов – сторон транзакции и многих других.

Для цитирования

Варбанова, Г. (2023). Правовая природа смарт-контрактов: договор или программный код? *Journal of Digital Technologies and Law*, *1*(4), 1028–1041. https://doi.org/10.21202/jdtl.2023.44

Содержание

Введение

Смарт-контракты представляют собой инструмент, весьма востребованный в современном праве и экономике. Однако, несмотря на его актуальность и необходимость, до сих пор отсутствует четкое регулирование смарт-контрактов как на национальном, так и на международном уровне.

Целью настоящего исследования является анализ правовой сущности смарт-контрактов и возможности их применения в гражданском и коммерческом обороте. Оно также призвано инициировать широкую дискуссию по вопросам, связанным с порядком применения технологий и необходимостью их своевременного регулирования. В данной работе мы стремились не только дать юридическое определение термина «смарт-контракт», но и выявить его характерные признаки, трактуемые в свете классического понимания договора. Тем самым мы хотим ответить на вопрос, является ли смарт-контракт, основанный на технологии блокчейна, собственно договором.

Для того чтобы проанализировать понятие «смарт-контракт», мы уточним особенности технологии блокчейна и принцип ее работы, а также напомним, что представляет собой классическое понимание договора, лежащее в основе гражданско-правовой системы. Это даст нам возможность ответить на вопрос, является ли смарт-контракт договором, порождает ли он права и как должны исполняться связанные с ним обязанности. Наконец, мы проанализируем особенности смарт-контрактов, связанные с привнесением в программный код специфического юридического языка.

1. Классическая теория контракта

Изучение правовой природы смарт-контрактов требует анализа теории контрактов и того, как возникают, развиваются и прекращаются договорные отношения. Этимология слова «контракт» раскрывает его основные особенности. Слово имеет латинское происхождение: существительное “contractus” происходит от глагола “contrahere”, что означает «соединять». Под контрактом часто понимают обязательство или ряд обязательств, связывающих стороны в рамках гражданско-правовой сделки. Эти обязательства подкрепляются принуждением со стороны государства, которое призвано обеспечить выполнение данного обещания, обязательства в рамках договорных отношений. Судебные иски в римском праве возникли как средство защиты нарушенного права. Они представляют собой процессуальный механизм, направленный на устранение последствий неисполнения договора. Это процессуальная возможность для сторон средствами государственного принуждения обеспечить тот результат, который они преследовали, заключая договор.

В начале XIX в. стала набирать популярность теория автономии воли. В ее основе лежит понимание того, что договор как таковой является следствием согласованной воли участников юридической сделки. Субъекты вольны вступать в договорные отношения добровольно, самостоятельно согласовывая параметры договора в противовес обязательствам, налагаемым законом, или обязательствам, вытекающим из деликта, утверждаемым с помощью специальной санкции государства. Согласно этой теории, роль контракта заключается в том, чтобы «содействовать свободе сторон в создании собственного частного права». Несмотря на то, что теория автономии воли имеет определенные недостатки, она оказала влияние на развитие современного договорного права и нашла свое выражение в принципе свободы договора согласно действующим правовым нормам.

Принцип автономии человеческой воли наиболее ярко проявляется в частноправовых отношениях, включая договорное право. В соответствии с этим принципом, субъекты вольны по взаимному согласию определять содержание правоотношения, в которое они желают вступить. Именно потому, что воля сторон является окончательной, суд при толковании договоров обязан искать их действительную общую волю и руководствоваться ею. Принцип автономии человеческой воли не должен считаться абсолютным, поэтому в ряде законодательств, в том числе и в болгарском, его применение связано с введением ограничений и других факторов для защиты как интересов сторон, так и публичных интересов. Так, согласно ст. 9 Закона Болгарии «Об обязательствах и договорах», стороны могут свободно определять содержание договора, но это содержание

не должно противоречить обязательным правовым нормам и требованиям морали. Например, Верховный кассационный суд Республики Болгария в своей судебной практике определяет пристойное поведение как моральные нормы, которым закон придает юридическое значение, поскольку правовые последствия их нарушения приравниваются к противоречию договора закону. Понятие пристойного поведения не включается в зафиксированные, систематизированные и конкретизированные правила; это скорее общие принципы или возникающие на их основе нормы, за соблюдением которых следит суд в рамках своей деятельности. Таким образом, любая из сторон свободна в принятии решения о вступлении или невступлении в конкретные договорные отношения с учетом обязательных правовых норм и требований морали. После достижения соглашения стороны могут решить, каково будет содержание заключаемого договора (объем прав и обязанностей) и когда его заключать. Стороны могут сами выбирать, заключать ли договор и в какой форме (Yossifova, 2019). Даже молчаливое волеизъявление может связывать стороны, и договор будет считаться заключенным, если законодатель не установит требование о форме. Требование формы – это требование ad solemnitatem. Отсутствие формы влечет за собой ничтожность договора. Даже если стороны составили документ, он не будет иметь той юридической силы, которой добивались стороны, если не имеет установленной законом формы. В целом болгарский законодатель придерживается мнения, что большинство договоров являются неформальными. Только в тех случаях, когда необходимо обеспечить правовую определенность, законодатель предусматривает обязанность составлять некоторые договоры в письменной или квалифицированной форме (нотариальное удостоверение или нотариальный акт). Следует отметить, что в соответствии с болгарским законодательством требование письменной формы считается выполненным, если составлен электронный документ, содержащий словесное заявление. Другими словами, когда законодатель требует, чтобы определенные договоры составлялись в письменной форме, это требование будет считаться выполненным, если составлен электронный документ, содержащий словесное заявление.

2. Блокчейн и концепция смарт-контракта

Идея смарт-контракта не нова (Sala-Climent, 2021; Ferreira, 2021; Fiorentino & Bartolucci, 2021; Eenmaa-Dimitrieva & Schmidt-Kessen, 2019). В области компьютерной науки и криптографии она зародилась еще в 1996 г., когда компьютерный инженер Ник Сабо представил свою идею самоисполняющегося программного кода. В основе идеи Сабо лежит компьютерный код, в котором реализована воля сторон и который при наступлении определенных условий сам себя исполняет таким образом, чтобы получить желаемый сторонами результат. Условия договора записываются непосредственно в строках кода, т. е. договор как таковой представляет собой программный код. Чтобы лучше проиллюстрировать свою идею, Сабо приводит пример с торговым автоматом. Покупатель напитка из торгового автомата имеет множество подразумеваемых прав потребителя, и на практике покупка напитка из торгового автомата представляет собой неформальный контракт, который с помощью программного кода обеспечивает каждого потребителя выбранным товаром по определенной цене. Таким образом, тот факт, что договор представлен

только в коде, как в случае со смарт-контрактами, не является особым препятствием для заключения неформального договора, исполнение которого автоматизировано с помощью программного кода. Несмотря на революционность идеи Сабо, она опередила свое время, поскольку технологии не достигли того уровня, который позволил бы ее массовое применение.

В 2008 г. Сатоши Накамото представил свою идею децентрализованной сети – блокчейна, а в 2014 г. Виталик Бутерин опубликовал книгу "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform" («Ethereum: Платформа для смарт-контрактов и децентрализованных приложений нового поколения»), которая возродила концепцию самоисполняющегося программного кода (Zhou et al., 2020). Смарт-контракт – это автоматизированный программный код, который сам по себе не является технологией создания искусственного интеллекта (Gallese, 2022). Самоисполнение смарт-контракта не связано с автоматизированной обработкой данных с целью принятия наиболее правильного решения при возникновении определенной ситуации. Оно предполагает автоматизированное исполнение – при наступлении события X выполняется действие Y; при этом смарт-контракт не имеет возможности путем анализа данных оценить, нужно продолжать исполнение или нет. Смарт-контракт призван снизить затраты и исключить фактор «доверия» при заключении контрактов. По сути, его задачами являются повышение скорости выполнения, существенное снижение затрат, отсутствие посредников и преодоление недоверия между сторонами. Смарт-контракт исполняется напрямую, не требуя каких-либо дополнительных действий или бездействия договаривающихся сторон: достаточно наличия условия, заданного в программном коде, и последствия сразу же наступят в правовом поле сторон. Основным преимуществом и в то же время недостатком технологии блокчейна является то, что она не позволяет модифицировать данные. Сам блок, а также цепочка блоков – это криптографический метод хранения данных в децентрализованной среде. Смарт-контракт хранится в децентрализованном реестре, поэтому для его хранения не требуется отдельного устройства, равно как и сторонам не требуется вести записи по этому контракту на локальных или иных технических средствах (Compagnucci et al., 2021). Транзакции в реестре связаны хронологически, что позволяет проследить запись от последнего до первого блока в цепи (первичного блока). После записи в блок цепочки блокчейн ее нельзя изменить (модифицировать) или удалить (Aleksieva et al., 2019), поскольку каждый блок цепочки блокчейна обладает целостностью, а каждая транзакция определена во времени – каждый блок содержит запись о транзакциях и информацию о временной метке последующего блока (Krumov & Atanasov, 2019). Это обеспечивает хронологическую связность информации в блокчейне и позволяет отследить ее до первичного блока. Это означает, что удаление или изменение (модификация) блока приведет к разрыву цепи блокчейна, что повлияет на процесс верификации блока. После заключения договора в форме смарт-контракта воля сторон не может быть изменена или модифицирована, т. е. если впоследствии их отношения претерпят изменения, сторонам придется заключать новый смарт-контракт, который прекратит действие уже существующего. Это, в свою очередь, ставит множество вопросов перед наукой и практикой.

3. Язык закона vs. программный код

С точки зрения науки и практики одним из основополагающих вопросов является перенесение («перевод») специфических терминов юридического языка в программный код смарт-контракта. При использовании смарт-контрактов необходимо учитывать специфические юридические термины, используемые в правовых нормах, и их корректную реализацию в программном коде смарт-контракта (Rizos, 2022). Это связано с тем, что, как уже было сказано, изменение или удаление записи в децентрализованном реестре невозможно, а точный перенос воли сторон в программный код имеет огромное значение, поскольку программный код должен отражать действительную волю сторон. Если воля сторон будет некорректно перенесена в программный код, смарт-контракт может самоисполниться, но его исполнение не будет соответствовать тому результату, на который рассчитывали стороны. В такой ситуации единственно возможным решением будет материализация действительной воли сторон в новой записи в виде нового смарт-контракта, поскольку исходная запись не может быть отредактирована или удалена. Появление новой записи зависит от того, согласятся ли на это стороны. Не исключено, что одна из сторон получила выгоду от своего некорректно реализованного в программном коде волеизъявления и поэтому предпочитает сохранить последствия в том виде, в котором они наступили, хотя такой результат отличается от согласованного сторонами. В этой ситуации понадобится вмешательство суда, который, интерпретируя волю сторон, должен будет выявить их действительную волю с учетом преддоговорных отношений. Однако подобная ошибка в воле сторон возможна и в классических договорных отношениях, которые возникают, развиваются и функционируют в форме обычного письменного документа.

Еще одной существенной особенностью смарт-контрактов является то, что на них распространяются общие нормы правового регулирования общественных отношений по различным видам сделок. При выборе тех или иных договорных отношений для закрепления в смарт-контракте стороны должны обратить внимание на то, предъявляется ли требование к форме договора и является ли оно требованием к его действительности или к его доказанности. Так, при отчуждении недвижимости сделка будет подчиняться общим правилам; чтобы такая сделка была действительной, она должна быть совершена в соответствии с требованием к форме – нотариальным актом (по законодательству Болгарии). Совершение сделки по распоряжению недвижимостью в форме смарт-контракта будет недействительным до тех пор, пока не будет соблюдено требование к форме – заключение нотариального акта. В таком случае можно подумать о преобразовании смарт-контракта и рассмотреть его в качестве предварительного договора купли-продажи недвижимости. Такое преобразование зависит от применимого права и от толкований, которые даются в судебной практике. С точки зрения болгарского права можно применить преобразование смарт-контракта с предметом купли-продажи недвижимого имущества согласно ст. 3 п. 2 Закона об электронных документах и электронных сертификационных услугах. Последний предусматривает, что письменная форма смарт-контракта будет считаться соблюденной только в том случае, если смарт-контракт содержит, помимо программного кода, словесное заявление сторон (Varbanova, 2020a).

4. Смарт-контракт как контракт по закону

С точки зрения действующего законодательства не существует никаких препятствий для заключения в форме смарт-контракта договорных отношений, для которых не предусмотрено соблюдение формы (в том числе квалифицированной) (Rühl, 2021). Согласно Регламенту (ЕС) № 910/2014 Европейского парламента и Совета от 23 июля 2014 г. об электронной идентификации и доверительных услугах для электронных транзакций на внутреннем рынке и отмене Директивы 1999/93/ЕО[1], это означает любой контент, хранящийся в электронной форме, в частности, текст, аудио-, видео- или аудиовидеозапись. Приведенный в Регламенте перечень не является исчерпывающим. Законодатель вполне логично посчитал, что бурное развитие технологий приведет к появлению новых технологических решений и понятие электронного документа будет иметь еще более широкую сферу применения (Varbanova, 2020b). Регламент непосредственно обязывает суды принимать электронные документы к рассмотрению. Суд не может игнорировать существование электронного документа, хотя, на первый взгляд, электронный документ не может быть воспринят судом так же, как классический письменный документ. Анализируя п. 35 ст. 3 Регламента, можно сделать вывод, что смарт-контракт должен восприниматься как электронный документ, хотя он и существует в виде программного кода. Таким образом, в приведенном выше примере сделки с недвижимостью эта недвижимость может быть токенизирована, но не с целью продажи, а, например, только для сдачи в аренду – это арендные отношения. Договор аренды является неформальным договором. С этой точки зрения доказать наличие такого договора будет гораздо проще, если он существует в виде смарт-контракта и токенизированного реального актива. Параметры арендных отношений будут прописаны в смарт-контракте – цена аренды, способ оплаты, срок и т. д. Благодаря сочетанию технологий интернета вещей и блокчейна оплата по договору может осуществляться автоматически, а при отсутствии поступления арендной платы на электронный кошелек владельца доступ к жилью может быть автоматически ограничен путем его блокировки с помощью технологических решений интернета вещей. В интернете вещей конечные устройства взаимодействуют друг с другом через глобальную сеть – Интернет. Применение блокчейна и интернета вещей зависит от воли сторон и от того, как эта воля будет реализована в смарт-контракте токенизированного реального актива.

Другая проблема, которая может возникнуть при использовании смарт-контрактов, заключается в том, что прецедентное право медленно реагирует на технологические достижения. Суды зачастую воспринимают в качестве документа только обычный документ, материализующий волю сторон на бумаге, в то время как смарт-контракт – это программный код, существующий в виде записи в децентрализованном реестре. Однако это не может быть препятствием для выполнения воли сторон, которые, особенно в неформальных договорных отношениях, вольны выбирать, как заключать договор и какие технологические решения при этом использовать.

---

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 On electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://clck.ru/36r5fJ

Идентификация субъектов – сторон сделки (Dimitrov et al., 2020) также может стать проблемой при использовании смарт-контрактов на основе технологии блокчейна. На данном этапе пока не существует единой правовой базы в отношении электронной идентификации, решение вопросов, связанных с идентификацией сторон, будет определяться применимым законодательством и тем, каким образом стороны хотят воспользоваться преимуществами технологии блокчейна. Так, при создании электронного кошелька некоторые поставщики услуг требуют верификации персональных данных его владельца (Zahariev, 2021), в том числе путем предоставления копии документа, удостоверяющего личность. Важно, чтобы каждую транзакцию с данного кошелька и на него можно было легко проследить и установить.

Для достижения целей контракта, а также ввиду того, что его исполнение может зависеть от наступления какого-либо события, не зависящего от воли сторон, технология позволяет использовать внешние источники – «оракулы» (Bomprezzi, 2021). Оракул – это независимый источник информации, находящийся вне блокчейна смарт-контракта (Basilan & Padilla, 2023). В области страхового права использование оракулов было бы крайне важно для получения информации, имеющей отношение к договору страхования и наступившему по нему страховому случаю, – информации о температуре, стихийном бедствии и т. д. Применение оракулов также возможно при использовании технологии блокчейна и смарт-контракта для обеспечения иска (Gromova, 2018): например, для блокировки определенного цифрового актива, который может быть разблокирован только при предоставлении внешней информации от оракула, например, при платеже по иску, обеспеченному цифровым активом (Nascimento & Martins, 2022). Проблема может возникнуть в том случае, если оракул предоставит неверную информацию, а смарт-контракт будет исполнен в соответствии с заложенным в него алгоритмом. В этих случаях потребуется вмешательство суда, но оно необходимо всякий раз, когда одна из сторон не выполняет своих обязательств, а смарт-контракт фактически исключает такую возможность. При наступлении события, заложенного в программном коде, смарт-контракт исполняет заложенный в него алгоритм, и такое исполнение не зависит от воли сторон.

Заключение

Исходя из проведенного анализа, можно дать определение смарт-контракта: это программный код с заранее заложенными сторонами условиями, на которых создаются, изменяются и прекращаются договорные отношения между ними. Исполнение контракта зависит не от действия или бездействия его сторон, а от заранее заданного условия (определенного факта, имеющего значение для сторон), при наступлении которого контракт самоисполняется. Воля сторон не может быть изменена или заменена именно в силу особого способа записи смарт-контракта в децентрализованном реестре. На основании проведенного анализа можно сделать вывод, что некоторые виды контрактов могут заключаться в форме смарт-контракта. При заключении смарт-контракта стороны должны соблюдать действующую нормативно-правовую базу, что может ограничить совершение некоторых сделок в форме смарт-контракта, особенно если законодатель установил

требование к форме при заключении отдельных видов договоров. Серьезной проблемой для юридической науки и практики является способ выражения воли сторон в смарт-контракте; это требует правильной интерпретации правовых понятий и включения их в программный код смарт-контракта.

Список литературы

Aleksieva, V., Valchanov, H., & Huliyan, A. (2019). Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services. *2019 International Conference on Biomedical Innovations and Applications (BIA)* (pp. 1–4). https://doi.org/10.1109/BIA48344.2019.8967468

Basilan, M. L. J. C., & Padilla, M. (2023). Assessment of teaching English Language Skills: Input to Digitized *Activities for campus journalism advisers. International Multidisciplinary Research Journal*, *4*(4), 118–130. https://doi.org/10.54476/ioer-imrj/245694

Bomprezzi, Ch. (2021). Implications of Blockchain-Based Smart Contracts on Contract Law. *Luxemburger Juristische Studien – Luxembourg Legal Studies*, *23*. https://doi.org/10.5771/9783748930068

Compagnucci, M. C., Fenwick, M., & Wrbka, S. (2021). The Uncertain Future of Smart Contracts. *Smart Contracts*, *12*, 11–12. https://doi.org/10.5040/9781509937059.ch-009

Dimitrov G., Petrivskyi V., Bychkova O., & Garvanova, M. (2020). Information technology for big data sensor networks stability estimation. *Information & Security*, *47*(1), 141–154. https://doi.org/10.11610/isij.4710

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M.-J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Fiorentino S., & Bartolucci S. (2021). Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities*, *117*, 103325. https://doi.org/10.1016/j.cities.2021.103325

Gallese, Ch. (2022). *Predictive Justice in Light of the New AI Act Proposal*. https://doi.org/10.2139/ssrn.4286023

Gromova, E. (2018). Smart contracts in Russia: an attempt to define the legal nature of smart contracts. *Law and Digital Economy*, *2*, 31–33. https://doi.org/10.17803/2618-8198.2018.02.2.031-033

Krumov, K., & Atanasov, A. (2019). The peculiarities of Blockchain technology. *Journal of Informatics and Innovative Technologies*, *1*, 3–6.

Nascimento, S. N. & Martins, D. G. D. (2022). Smart Contracts: Security Issues and Further Development in Brazil. *International Journal of Law in Changing World*, *1*(2), 26–45. https://doi.org/10.54934/ijlcw.v1i2.22

Rizos, E. (2022). A contract law approach for the treatment of smart contracts' 'bugs'. *European Review of Private Law*, *30*(5), 775–802. https://doi.org/10.54648/erpl2022037

Rühl, G. (2021). Smart (legal) contracts, or: Which (contract) law for smart contracts? *Blockchain, Law and Governance*, *8*, 159–180. https://doi.org/10.1007/978-3-030-52722-8_11

Sala-Climent, M. T. (2021). Smart contracts – technological, business and legal perspectives. *European Review of Contract Law*, *17*(4), 385–389. https://doi.org/10.1515/ercl-2021-2033

Varbanova, G. (2020a). *Legal regime of electronic documents*. Dangrafik, Varna.

Varbanova, G. (2020b). Smart contract and challenges to law. In *The law and the business in the contemporary society: Conference Proceedings of the 3rd National Scientific Conference* (pp. 359–364). https://doi.org/10.36997/lbcs2020.359

Yossifova, T. (2019). *Effect of Contracts Vis-à-vis Individuals*. Sibi, Sofia.

Zahariev, M. (2021). *Protection of personal data during video surveillance, Intellectual property in the new (ab) normal*. Sofia, AzBuki.

Zhou, Z., Li, R., Cao, Y., Zheng, L., & Xiao, H. (2020). Dynamic performance evaluation of blockchain technologies. *IEEE Access*, *8*, 217762–217772. https://doi.org/10.1109/access.2020.3040875

Информация об авторе

Варбанова Гергана – PhD, ассистент кафедры правоведения, Университет национального и мирового хозяйства, арбитр Арбитражного суда BIA
Адрес: Болгария, г. Варна, ул. Дрин, 10
E-mail: gergana@varbanova.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
WoS Researcher ID: https://www.webofscience.com/wos/author/record/37781549
Google Scholar ID: https://scholar.google.com/citations?user=02-0uFYAAAAJ

Конфликт интересов

Автор является членом редакционной коллегии журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 25 мая 2023 г.
Дата одобрения после рецензирования – 7 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.44

Legal Nature of Smart Contracts: Contract or Program Code?

Gergana Varbanova

University of National and World Economy;
Arbitration Court of the BIA
Varna, Bulgaria

Keywords

blockchain,
civil law,
commercial law,
contract law,
contract,
digital technologies,
information technologies,
law,
program code,
smart contract

Abstract

Objective: due to the rapid technological changes, digital economy and contractual relations determine law transformation and legislation development towards adaptation to prospective spreading and application of smart contracts in civil and commercial turnover. In this regard, the study focuses on determining the legal essence of smart contracts as a fundamental step towards the development of their timely and clear regulation.

Methods: the research is based on the methodology of formal-legal and comparative legal analysis. It compares the current Bulgarian legislation with supranational legal sources and identifies the characteristic features of smart contracts as demanded instruments necessary for modern law and economy. The article also compares them with the classical understanding of contracts, making it possible to understand and define the nature of smart contracts more accurately.

Results: it was determined that a smart contract is a software code in which the parties predetermine conditions under which the contractual relationship between them is created, modified and terminated. The research proved that the contract execution does not depend on the action or inaction of its parties, but rather on the occurrence of a predetermined condition (a certain fact relevant to the parties) under which the contract must self-execute. It was substantiated that the will of the parties cannot be changed or replaced because of the special way in which the smart contract is recorded in a distributed ledger. It is found that the fundamental problem of transferring the will from the legal language to the program code of the smart contract persists: if the will of the parties is incorrectly transferred to the program code, the smart contract may self-execute, but its execution will not be the result that the parties counted on.

Scientific novelty: the analysis made it possible to compare the current national (Bulgarian) legislation and supranational (European) law. It revealed the vagueness of smart contracts regulation, both at the national and international level, and identified a number of issues in need of scientific and legal interpretation, which refer to the legal nature of smart contracts in view of the self-executing program code concept.

Practical significance: the study can serve as a basis for further development of legislation towards its adaptation to the prospects of smart contracts spreading and application in civil and commercial turnover. It also allows an in-depth analysis of the smart contracts practice referring to such unsolved problems as accurate transference of the parties' will to the program code (translation of specific terms from the legal language into the smart contract program code), electronic identification of subjects – parties to the transaction and many other issues.

For citation

Varbanova, G. K. (2023). Legal Nature of Smart Contracts: Contract or Program Code? *Journal of Digital Technologies and Law, 1*(4), 1028–1041. https://doi.org/10.21202/jdtl.2023.44

References

Aleksieva, V., Valchanov, H., & Huliyan, A. (2019). Application of Smart Contracts based on Ethereum Blockchain for the Purpose of Insurance Services. *2019 International Conference on Biomedical Innovations and Applications (BIA)* (pp. 1–4). https://doi.org/10.1109/BIA48344.2019.8967468

Basilan, M. L. J. C., & Padilla, M. (2023). Assessment of teaching English Language Skills: Input to Digitized *Activities for campus journalism advisers. International Multidisciplinary Research Journal*, *4*(4), 118–130. https://doi.org/10.54476/ioer-imrj/245694

Bomprezzi, Ch. (2021). Implications of Blockchain-Based Smart Contracts on Contract Law. *Luxemburger Juristische Studien – Luxembourg Legal Studies*, *23*. https://doi.org/10.5771/9783748930068

Compagnucci, M. C., Fenwick, M., & Wrbka, S. (2021). The Uncertain Future of Smart Contracts. *Smart Contracts*, *12*, 11–12. https://doi.org/10.5040/9781509937059.ch-009

Dimitrov G., Petrivskyi V., Bychkova O., & Garvanova, M. (2020). Information technology for big data sensor networks stability estimation. *Information & Security*, *47*(1), 141–154. https://doi.org/10.11610/isij.4710

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M.-J. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Fiorentino S., & Bartolucci S. (2021). Blockchain-based smart contracts as new governance tools for the sharing economy. *Cities*, *117*, 103325. https://doi.org/10.1016/j.cities.2021.103325

Gallese, Ch. (2022). *Predictive Justice in Light of the New AI Act Proposal*. https://doi.org/10.2139/ssrn.4286023

Gromova, E. (2018). Smart contracts in Russia: an attempt to define the legal nature of smart contracts. *Law and Digital Economy*, *2*, 31–33. https://doi.org/10.17803/2618-8198.2018.02.2.031-033

Krumov, K., & Atanasov, A. (2019). The peculiarities of Blockchain technology. *Journal of Informatics and Innovative Technologies*, *1*, 3–6.

Nascimento, S. N. & Martins, D.G. D. (2022). Smart Contracts: Security Issues and Further Development in Brazil. *International Journal of Law in Changing World*, *1*(2), 26–45. https://doi.org/10.54934/ijlcw.v1i2.22

Rizos, E. (2022). A contract law approach for the treatment of smart contracts' 'bugs'. *European Review of Private Law*, *30*(5), 775–802. https://doi.org/10.54648/erpl2022037

Rühl, G. (2021). Smart (legal) contracts, or: Which (contract) law for smart contracts? *Blockchain, Law and Governance*, *8*, 159–180. https://doi.org/10.1007/978-3-030-52722-8_11

Sala-Climent, M. T. (2021). Smart contracts – technological, business and legal perspectives. *European Review of Contract Law*, *17*(4), 385–389. https://doi.org/10.1515/ercl-2021-2033

Varbanova, G. (2020a). *Legal regime of electronic documents*. Dangrafik, Varna.

Varbanova, G. (2020b). Smart contract and challenges to law. In *The law and the business in the contemporary society: Conference Proceedings of the 3rd National Scientific Conference* (pp. 359–364). https://doi.org/10.36997/lbcs2020.359

Yossifova, T. (2019). *Effect of Contracts Vis-à-vis Individuals*. Sibi, Sofia.

Zahariev, M. (2021). *Protection of personal data during video surveillance, Intellectual property in the new (ab) normal*. Sofia, AzBuki.

Zhou, Z., Li, R., Cao, Y., Zheng, L., & Xiao, H. (2020). Dynamic performance evaluation of blockchain technologies. *IEEE Access*, *8*, 217762–217772. https://doi.org/10.1109/access.2020.3040875

Author information

Gergana Varbanova – PhD, Assistant Professor at the Department of Legal Studies, University of National and World Economy, Arbitrator of the Arbitration Court of the BIA
Address: 10 Drin Street, Varna, Bulgaria
E-mail: gergana@varbanova.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
WoS Researcher ID: https://www.webofscience.com/wos/author/record/37781549
Google Scholar ID: https://scholar.google.com/citations?user=02-0uFYAAAAJ

Conflict of interest

The author is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 25, 2023
Date of approval – October 7, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47:339
EDN: https://elibrary.ru/gvbwbi
DOI: https://doi.org/10.21202/jdtl.2023.45

Смарт-контракты в международной торговле: европейские правовые стратегии преодоления трудностей

Тарика Дишани Ламаппулаге Донн

Гринвичский университет
г. Лондон, Великобритания

Ключевые слова

алгоритмический код,
компьютерная программа,
международная торговля,
право,
смарт-контракт,
технологии блокчейн,
цифровизация,
цифровое соглашение,
цифровые технологии,
электронная форма

Аннотация

Цель: присущая смарт-контрактам автоматизация делает их привлекательным инструментом для применения в сфере глобальной торговли, особенно с целью автоматизации транзакций. Прогнозируемая перспектива окажет серьезное влияние на международные экономические отношения и трансформацию правил международной торговли, что фокусирует настоящее исследование на выявлении возможностей трансформации указанных правил и принимаемых европейскими странами политико-правовых стратегий внедрения смарт-контрактов в международную торговлю.

Методы: исследование текущего состояния регулирования международной торговли в условиях процессов цифровизации, оцифровки контрактов и распространения смарт-контрактов основывается на совокупности формально-юридического и сравнительно-правового методов, позволяющих изучить правила международной торговли, проанализировать в сравнении политико-правовые позиции Великобритании и Европейского союза по вопросу внедрения смарт-контрактов в международную торговлю, а также спрогнозировать юридические последствия использования смарт-контрактов в указанной области (прогностический метод).

Результаты: исследование показывает, что распространение смарт-контрактов имеет существенные последствия для международной торговли и ее регулирования. Обладая многочисленными преимуществами,

такими как повышенная эффективность, снижение затрат и широкая доступность, они при согласовании традиционных правовых принципов с цифровой средой могут привести к юридическим проблемам, в частности, касающимся аутентификации субъектов, возможности принудительного исполнения от конкретных обстоятельств дела, вопросов юрисдикции.

Научная новизна: имеющаяся литература по вопросам трансформации регулирования международной торговли в условиях процессов цифровизации и распространения смарт-контрактов дополняется результатами сравнительного анализа правовых позиций, имеющихся на европейском правовом пространстве и выработанных на основе проблем, уроков и достижений при внедрении смарт-контрактов в международную торговлю.

Практическая значимость: понимание юридических последствий смарт-контрактов имеет важное значение для предприятий, участвующих в международной торговле. Исследование дает представление о правовых позициях Великобритании и Европейского союза, на основе которых можно выработать рекомендации компаниям, ориентирующимся в цифровом ландшафте. Директивные органы также могут извлечь пользу из полученных результатов для разработки соответствующих правовых актов, которые уравновешивают преимущества смарт-контрактов с необходимостью правовой определенности и защитой в международной торговле.

Для цитирования

Ламаппулаге Донн, Т. Д. (2023). Смарт-контракты в международной торговле: европейские правовые стратегии преодоления трудностей. *Journal of Digital Technologies and Law*, *1*(4), 1042–1057. https://doi.org/10.21202/jdtl.2023.45

Содержание

Введение

Смарт-контракты – это цифровые соглашения, которые могут выполняться автономно, позволяя сторонам открыто и бесконфликтно передавать друг другу цифровые и физические активы и другие ценности (Hewa et al., 2021). Американский специалист Ник Сабо, разработчик цифровой валюты Bit Gold, в 1998 г. определил смарт-контракт как «компьютерный протокол транзакций, выполняющий условия контракта»[1]. Сатоши Накамото также обосновал идею смарт-контракта в 2008 г. в статье «Bitcoin: A Peer-to-Peer Electronic Cash System» [Биткоин: одноранговая электронная денежная система] (Nakamoto, 2008). Количество биткоинов в обращении и полномочия по созданию и перемещению биткоинов отслеживаются и контролируются распределенной базой данных, которая работает на программном обеспечении смарт-контрактов. По словам Ника Сабо, как торговые автоматы заменили продавцов-людей, так и смарт-контракты способны вытеснить посредников в различных отраслях.

При необходимости заключить сложную сделку с участием значительной суммы денег мы, как правило, обращаемся за консультацией к юристу или нотариусу, оплачиваем услуги этого специалиста, а затем ожидаем выполнения поставленной задачи и соблюдения условий договора (Vatiero, 2023). Пока юрист не удостоверится, что все бумаги оформлены правильно, мы не получим доступа к денежным средствам или имуществу. Однако, поместив биткоин в реестр, можно немедленно получить акт, контракт, продукты, водительские права – все, что предусмотрено смарт-контрактом. Смарт-контракты – это программный посредник между потребителем и блокчейн-хранилищем (Ferreira, 2021). Смарт-контракты исполняют алгоритм, необходимый для предоставления сложной услуги по запросу клиента, включая такие действия, как проверка статуса и идентификации и выполнение задачи. Они позволяют пользователям хранить данные в блокчейн-хранилище и получать к ним доступ без необходимости выполнять поиск. Доступ к основным структурам блокчейн-хранилища предоставляет компьютерный интерфейс (Bandara et al., 2019).

На протяжении столетий Великобритания поддерживает стабильность своей правовой системы. В настоящее время она входит в число стран, которые исследуют и внедряют смарт-контракты. В ноябре 2021 г. член парламента Доминик Рааб, занимающий посты лорда-канцлера и министра юстиции, представил правительству предложение по смарт-контрактам, которое было расценено как прогрессивная мера[2]. Страны Европейского союза в последние годы также предпринимают усилия, связанные со смарт-контрактами. В данной работе основное внимание уделяется процессу внедрения смарт-контрактов в Великобритании и ЕС, а также анализу их влияния на регулирование международной торговли в условиях цифровизации. Исследование также направлено на оценку правовой базы Великобритании и ЕС в отношении смарт-контрактов. Цель работы – оценить совместимость существующей законодательной базы с технологией смарт-контракта и изучить проблемы

1 Zapotochnyi, A. (2022, October 19). What are smart contracts? Blockgeeks. https://clck.ru/36kyjY

2 The Law Commission. (2021). Smart legal contracts Advice to Government. https://goo.su/FohUZ

и достижения, возникшие в процессе внедрения смарт-контрактов в международную торговлю (Zhang et al., 2023).

В работе использовался доктринальный подход, который предполагает, прежде всего, анализ правовых источников, таких как статуты, прецеденты и юридические комментарии (Fatima, 2023). Данный подход позволил провести комплексный анализ существующей правовой базы смарт-контрактов в Великобритании и ЕС. В ходе исследования были проанализированы соответствующие источники, такие как научная литература, правительственные отчеты и отраслевые публикации, что позволило получить представление о нормативно-правовой базе, вариантах ее использования, преимуществах, проблемах и уроках, извлеченных из опыта применения смарт-контрактов в Великобритании. Анализ был направлен на выявление любых правовых проблем, стоящих на пути внедрения смарт-контрактов в Великобритании, и любых правовых решений, которые могут быть реализованы для устранения этих проблем.

Кроме того, методология данной работы включает качественное исследование, которое предполагает изучение и понимание значения, опыта и перспектив отдельных лиц или групп с помощью таких методов, как наблюдение и анализ документов.

1. Как работают смарт-контракты?

Существует несколько видов смарт-контрактов, например, юридические смарт-контракты и рикардианские контракты. Смарт-контракты могут использоваться в различных бизнес-процессах, при торговле активами и в других видах сделок, детали которых определяются участвующими сторонами в зависимости от уровня их сотрудничества и желаемых результатов (Ji et al., 2023; Ante, 2021). Любое событие или ситуация, например изменение показателей финансового рынка или GPS-координат пользователя, может инициировать исполнение смарт-контракта либо самими сторонами контракта, либо от их имени (Gunay & Kaskaloglu, 2022; Wang et al., 2023a). Когда требования компьютерной программы выполнены, она запускается автоматически без участия человека. Коммуникация между участниками смарт-контракта может быть заверена и безопасно передана в зашифрованном виде (Kirli et al., 2022). В настоящее время наиболее распространенным инструментом для создания и реализации смарт-контрактов является Ethereum, но то же самое могут делать и другие криптовалюты на основе блокчейна, такие как EOS, Neo, Tezos, Tron, Polkadot и Algorand (Sathiyamurthy & Kodavali, 2023; Liu et al., 2023). После выполнения смарт-контракта каждый сервер сети обновляет запись, отражающую рабочее состояние сети на данный момент. После загрузки в блокчейн и верификации документ уже нельзя изменить. Проблема достоверности международных торговых контрактов может быть эффективно решена за счет использования неизменяемых и распределенных свойств блокчейна (Pishdad-Bozorgi & Han Yoon, 2022).

Виртуальная машина Ethereum Virtual Machine (EVM) управляет исполнением смарт-контрактов на блокчейне Ethereum в рамках платформы Ethereum (Liu et al., 2022; Wang et al., 2023b). Перед запуском совершенного смарт-контракта на конкретных блокчейнах необходимо внести плату за транзакцию – «оплату за газ». Чем сложнее операции смарт-контракта, тем выше будет «плата за газ». Это делается для защиты виртуальной машины Ethereum от возможных перегрузок, вызванных исполнением слишком сложных или многочисленных смарт-контрактов

(Eenmaa-Dimitrieva & Schmidt-Kessen, 2019). «Газ» можно образно представить как движущую силу, которая исполняет смарт-контракты Ethereum. Недостаток газа может помешать сети проводить транзакции. Каждая транзакция связана с платой за газ, и запуск транзакций зависит от распределения контрактов по сети. Для выполнения транзакций требуется значительный объем вычислительных ресурсов. Вычисления, необходимые для проведения транзакции, определяют размер платы за газ[3].

2. История развития смарт-контрактов в Великобритании и ЕС

2.1. Подход Великобритании

В рамках государственной Программы «Innovate UK» 3 августа 2016 г. в Великобритании начались продажи технологии блокчейн как услуги (Blockchain as a service, BaaS). Возможность применения технологии блокчейн рассматривается Налогово-таможенной службой Великобритании, как и других технических средств для совершенствования налоговых, таможенных и акцизных систем. В мае 2016 г. Парламентское бюро по вопросам науки и техники (Parliamentary Office of Science and Technology, POST) подготовило краткий отчет о финансовых технологиях, уделив особое внимание четырем инновационным областям, одной из которых была технология распределенного реестра (DLT). В январе 2018 г. POST выпустило документ под названием «Темы, представляющие интерес», в котором технология распределенного реестра (DLT) была определена как область, требующая дальнейших исследований. Министерство труда и пенсионного обеспечения Великобритании совместно с компанией GovCoin провело исследование потенциала технологии блокчейна для совершенствования социального обеспечения (Hughes et al., 2018). В 2019 г. Рабочая группа по вопросам юрисдикции (UK Jurisdiction Taskforce, UKJT) пришла к выводу, что возможность принудительного исполнения смарт-контрактов зависит от конкретных обстоятельств дела. Перед Комиссией по законодательству была поставлена задача оценить надежность существующей правовой и законодательной баз в свете требований к управлению смарт-контрактами, выделить любые неопределенности и при необходимости предложить новые и/или обновленные законы (Ferro et al., 2023). Однако, несмотря на все законодательные усилия, исследований по оценке эффективности этих мер до сих пор недостаточно (Blaszczyk, 2023).

2.2. Подход ЕС

11 апреля 2018 г. двадцать две страны Европы подписали договор о Европейском блокчейн-партнерстве (European Blockchain Partnership, EBP). В эту коалицию вошли Нидерланды, Германия, Франция, Норвегия, Испания и другие страны. По словам Марии Габриэль, еврокомиссара по цифровой экономике и обществу, блокчейн – это прекрасная возможность для Европы и стран-участниц пересмотреть свои информационные системы, стимулировать доверие к пользователям

[3] Frankenfield, J. (2022, September 27). Gas (Ethereum): How Gas Fees Work on the Ethereum Blockchain. Investopedia. https://clck.ru/36kytz

и безопасность персональных данных, развивать новые возможности для бизнеса и формировать новые области лидерства в интересах граждан, государственных служб и бизнес-структур.

Понятие «е-резидент» впервые возникло в 2014 г. в Эстонии. Люди со всего мира участвовали в цифровой программе, становясь цифровыми резидентами и регистрируя компании в Эстонии. В противовес этой ситуации возникло движение блокчейна, направленное на децентрализацию услуг. Логичным шагом явилось объединение программы «Электронный резидент Эстонии» с технологией блокчейна. В настоящее время программа E-Estonia работает на базе Ethereum. Официальная подготовка к проведению ICO в Эстонии пока находится в стадии разработки. Чтобы добавить новое измерение и удобство в программу е-резидентства, была создана валюта ESTcoin. В будущем экосистема е-резидентства должна быть усовершенствована (Kim, 2023).

14 марта 2023 г. Европейский парламент одобрил новые меры контроля данных в рамках масштабного законопроекта о конфиденциальности данных. Законопроект призван решить проблему защиты цифровой частной жизни, при этом не создавая препятствий для инноваций (Perez & Zeadally, 2023). Согласно новому положению Закона о данных, все смарт-контракты теперь должны иметь «аварийный выключатель». В случае нарушения безопасности специалисты в сфере информационных технологий используют метод «аварийного выключателя» для немедленного отключения системы. При обнаружении критического дефекта или атаки «выключатель» в коде смарт-контракта может либо немедленно прекратить его действие, либо приостановить его, исправить нарушения и запустить контракт заново[4].

3. Правовые основы международной торговли в Великобритании и ЕС

3.1. Политика международной торговли в Великобритании

Процветание экономики как Великобритании, так и мира в целом зависит от наличия торговли, свободной от ограничений и предвзятости. Соответственно, рост заработной платы ведет к повышению доступности более широкого спектра товаров и услуг по разумным ценам, что приводит к увеличению доходов населения, особенно наиболее уязвимых его слоев. Более 50 % валового внутреннего продукта Великобритании приходится на международную торговую деятельность. Великобритания официально вышла из состава ЕС 31 января 2020 г. по результатам референдума, проведенного в июне 2016 г. В 2018 г. был применен Закон о выходе из Европейского союза, с тем чтобы ассимилировать нормативные акты ЕС в правовую базу страны. Это было сделано путем замены ссылок на организации, законы и нормативные акты ЕС соответствующими ссылками на британские институты с целью обеспечения преемственности правового регулирования и процессов и предотвращения возможных сбоев. После событий 1 января 2021 г. можно констатировать, что нормативно-правовая база Великобритании и ЕС оказалась практически аналогичной. Однако следует отметить, что Великобритания теперь обладает правом изменять свои законы и нормы, не обращаясь за консультацией к ЕС. Недавно Великобритания и ЕС утвердили Соглашение о торговле и сотрудничестве (UK-EU Trade

[4] Shamai, S. (2023, March 29). The EU's Smart Contract 'Kill Switch' Mandate Won't Kill Crypto. Coindesk. https://clck.ru/36kywE

and Cooperation Agreement, TCA), и оно вступило в силу 1 января 2021 г. Это новое торговое соглашение гарантирует, что обе стороны будут по-прежнему иметь доступ на рынки друг друга без введения тарифов и квот, а также позволяет создание независимой нормативно-правовой базы для Великобритании и ЕС (Buigut & Kapar, 2023). Согласно TCA, каждая из сторон может предлагать изменения в соглашение в части обязательств по доступу на рынки, в случае если возникнут существенные торговые последствия из-за различий во внутренней нормативной базе[5].

Имплементация Типового закона о трансграничной несостоятельности (ЮНСИТРАЛ) в Великобритании была осуществлена посредством Положения о трансграничной несостоятельности 2006 г. Скорейшее рассмотрение Великобританией вопроса об имплементации этих мер послужит наглядным свидетельством ее неизменной приверженности взаимному сотрудничеству и соблюдению мировых стандартов. Смарт-контракты имеют юридическую силу в соответствии с Конвенцией ООН о международной купле-продаже товаров (Convention on Contracts for the International Sale of Goods, CISG), поскольку удовлетворяют критериям оферты и акцепта, указанным в ст. 14 и 18. При этом следует отметить, что Великобритания остается одной из немногих промышленно развитых стран мира, до сих пор не внедривших данную Конвенцию. Это объясняется несколькими факторами, в частности, тем, что Конвенция в большей степени тяготеет к гражданскому праву, отсутствует достаточная мотивация со стороны бизнеса, выступающего за ее ратификацию, и потенциально снижена значимость Лондона как центра коммерческого арбитража (Hoekstra, 2021).

3.2. Политика международной торговли в ЕС

Торговая и инвестиционная политика Европейского союза определяет его торговые и инвестиционные отношения со странами, не входящими в ЕС. Торговля со странами за пределами ЕС происходит по нормам ЕС, а не по национальным нормам отдельных стран-членов. Институты ЕС отвечают за разработку законодательства по вопросам торговли, а также участвуют в переговорах и заключении глобальных торговых соглашений. ЕС придерживается основополагающих принципов Всемирной торговой организации. В июне 2018 г. на фоне роста глобальной напряженности в сфере торговли Европейский совет подчеркнул важность сохранения и укрепления многосторонней системы, функционирующей на основе установленных правил. ЕС выразил готовность повышать эффективность работы Всемирной торговой организации в сотрудничестве с другими странами, разделяющими эту позицию. Торговые соглашения сложны по своей природе, поскольку основываются на юридических документах, охватывающих широкий спектр деятельности – от сельского хозяйства до интеллектуальной собственности. Однако в них прослеживается множество основополагающих принципов, которые являются общими для всех[6].

---

5 GOV.UK. (2018). UK trade policy: A guide to new trade legislation. https://clck.ru/ZBrtd

6 European Commission. Making Trade Policy. https://clck.ru/36kz2m

4. Цифровизация контрактов в Великобритании и ЕС

4.1. Развитие законодательства в Великобритании

В соответствии с Тринадцатой программой реформирования законодательства по указанию лорда-канцлера Комиссия по законодательству должна была провести исследование и анализ в области правовых смарт-контрактов. В ноябре 2019 г. Рабочая группа по вопросам юрисдикции опубликовала официальное заявление по криптоактивам и смарт-контрактам. В нем указывалось, что смарт-контракты обладают потенциалом для создания юридически связывающих обязательств, которые могут быть принудительно исполнены в соответствии с их условиями. Впоследствии Министерство юстиции обратилось к Комиссии по законодательству с просьбой провести всестороннее изучение существующей правовой базы, касающейся смарт-контрактов. С этой целью Комиссия провела дополнительный анализ, направленный на выяснение любых вопросов или пробелов в действующем законодательстве и определения области любых дополнительных исследований, которые могут потребоваться в настоящее время или в будущем.

При возникновении разногласий по договорам суды опираются на специальное разъяснение, в котором дается их толкование смарт-контрактов. Согласно этому документу, суды оценивают значение программного кода, используемого в договоре, с точки зрения программиста, обладающего опытом в соответствующей области и действующего рационально, а также принимают во внимание всю соответствующую контекстуальную информацию, которая была доступна сторонам на момент заключения договора. По мнению Комиссии по законодательству, необходимо подвергать толкованию даже интеллектуальные правовые договоры, полностью состоящие из кода, поскольку существует вероятность расхождения между предполагаемым смыслом кода и его фактическим исполнением. Это связано с различием между семантической интерпретацией кода и его практической реализацией. Включение кода в систему толкования потенциально может привести к возникновению проблем с интерпретацией. Комиссия рекомендует использовать для оценки обычный критерий, согласно которому толкование термина основывается на понимании и осведомленности лица, обладающего опытом в соответствующей области (Durovic & Willett, 2023). Этот метод интерпретации договоров в настоящее время преобладает.

Трудно переоценить значение определенности с юридической точки зрения. Примечательно, что английское право признано способным инкорпорировать смарт-контракты. Это гарантирует защиту сторон международных торговых соглашений, заключенных посредством компьютерных технологий, в случаях, когда смарт-контракт подпадает под действие английского права. Кроме того, в докладе Комиссии по законодательству приводятся факторы, которые должны учитывать договаривающиеся стороны, что будет особенно актуально для лиц, работающих в сфере децентрализованных финансов.

4.2. Развитие законодательства в ЕС

Законодательство в области смарт-контрактов и интернета вещей было одобрено Европейским парламентом 14 марта 2023 г. в рамках Закона о данных подавляющим большинством голосов (500 голосов за и 23 против). Его цель – содействовать развитию бизнес-моделей, способствующих появлению новых отраслей и возможностей

для трудоустройства. Статья 30 Закона о данных содержит положения, касающиеся фундаментальных предпосылок, связанных со смарт-контрактами для обмена данными (Casolari et al., 2023). Начиная с 2024 г. корпорации должны соблюдать новые правила при предложении услуг или товаров потребителям, находящимся на территории ЕС. Содержание закона было одобрено Европейским парламентом и в настоящее время находится на стадии обсуждения. После утверждения закона последует 12-месячный период его внедрения.

Реализация Закона о данных требует создания эффективных механизмов прекращения исполнения контрактов. Эти механизмы могут включать в себя внутренние функции, позволяющие отменить контракт или дающие команду по его прекращению. Необходимо четко определить обстоятельства, которые являются основанием для отмены или прекращения действия смарт-контракта. В сфере информационных технологий администраторы часто используют механизм «аварийного выключателя» в качестве средства прекращения работы устройства, сети или программного обеспечения в ответ на угрозу безопасности (Philip & Saravanaguru, 2022). В контексте смарт-контрактов «выключатель» должен либо расторгнуть контракт, либо инициировать процесс его прекращения, коррекции и последующего перезаключения, если обнаружится существенная уязвимость или нарушение (Chu et al., 2023).

Закон о данных – это важнейшая инициатива, направленная на повышение доступности данных в соответствии с принципами и правилами ЕС. Он представляет собой фундаментальный компонент европейской стратегии в области данных. Его принятие будет в значительной степени способствовать достижению цели цифровой трансформации, обозначенной в проекте «Цифровое десятилетие». Оценка соответствия основным принципам будет проводиться разработчиком или провайдером смарт-контрактов. Впоследствии они должны будут предоставить декларацию соответствия ЕС и нести ответственность за соответствие существенным требованиям. Определение термина «ответственность» в данном контексте остается неоднозначным, поэтому неясно, будут ли пользователи смарт-контракта нести какую-либо гражданскую ответственность. В случае несоответствия смарт-контракта нормативным требованиям последствия будут определяться законодательством соответствующего государства – члена ЕС.

4.3. Позиция ВТО

ВТО опубликовала несколько отчетов в области смарт-контрактов и соответствующих технологий, в которых отмечалось, что присущая смарт-контрактам автоматизация делает их привлекательным инструментом для использования в сфере глобальной торговли, в частности для автоматизации сделок. Использование смарт-контрактов порождает юридические проблемы, требующие тщательного рассмотрения, в частности, в отношении вопросов исполнения контрактов и правовой ответственности в случае ошибок кодирования (Papadouli & Papakonstantinou, 2023). Кроме того, смарт-контракты – это программные приложения, которые, как и любой код, могут содержать непреднамеренные ошибки. Безопасность экосистемы блокчейна может быть уязвима, прежде всего, на уровне смарт-контрактов, а также на уровне пользовательского интерфейса,

включающего такие устройства для доступа в Интернет, как мобильные телефоны, планшеты или компьютеры[7]. В докладе WCO/WTO о подрывных технологиях (Study Report on Disruptive Technologies) также показано, как смарт-контракты могут использоваться в международной торговле и для поставки товаров[8].

Таким образом, очевидно, что Всемирная торговая организация в настоящее время рассматривает возможность использования смарт-контрактов в международной торговле. Эта технология экономит время и деньги, что может послужить стимулом для участников рынка к более активному ее использованию.

Заключение

Смарт-контракты содержат программный код, который автоматически исполняет соглашение или его часть. Даже смарт-контракты, полностью состоящие из программного кода, могут быть действительны в соответствии с Конвенцией ООН о международной купле-продаже товаров, поскольку они удовлетворяют условиям оферты и акцепта, содержащимся в ст. 14 и 18 данной Конвенции.

В настоящее время Великобритания и ЕС применяют прогрессивный подход к смарт-контрактам. Великобритания адаптирует существующую правовую базу для регулирования смарт-контрактов и возникающих в связи с этим конфликтов, в то время как ЕС пытается регулировать исполнение юридических контрактов с помощью нового законодательства. ВТО также продолжает технико-экономические исследования, касающиеся смарт-контрактов и связанных с ними технологий. Таким образом, можно сделать вывод, что в настоящее время цифровизация контрактов не будет иметь значительного влияния на правила международной торговли. Однако, поскольку смарт-контракты все еще являются развивающейся технологией, может возникнуть необходимость в разработке нового законодательства для решения вопросов, которые появятся в будущем.

Список литературы

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Bandara, E., Ng, W. K., Ranasinghe, N., & De Zoysa, K. (2019). Aplos: Smart Contracts made smart. In J. F. Ashish, Gh. R. Oliveira, P. L. Zhou (Eds.), *Communications in Computer and Information Science* (pp. 431–445). https://doi.org/10.1007/978-981-15-2777-7_35

Blaszczyk, M. (2023). *Smart contracts, Lex cryptographia, and transnational contract theory*. SSRN. https://doi.org/10.2139/ssrn.4319654

Buigut, S., & Kapar, B. (2023). How did Brexit impact EU trade? Evidence from real data. *The World Economy*, *46*(6), 1566–1581. https://doi.org/10.1111/twec.13419

Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. *Digital Society*, *2*(1). https://doi.org/10.1007/s44206-023-00038-2

Chu, H., Zhang, P., Dong, H., Xiao, Y., Shunhui, J., & Wenrui, L. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*(107221). https://doi.org/10.1016/j.infsof.2023.107221

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in Consumer Contracts: Machines as servants, not masters. *The Modern Law Review*. https://doi.org/10.1111/1468-2230.12817

7 Ganne, E. (2018). Can Blockchain Revolutionize International Trade? https://clck.ru/36kz6N

8 WTO and World Customs Organization. WCO/WTO Study Report on Disruptive Technologies. (2022). https://clck.ru/36kzCD

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Fatima, S. (2023). Employability of a Research Method and Methodology in a Socio-Legal Study. *Global Social Sciences Review*, *VIII*(I), 341–351. https://doi.org/10.31703/gssr.2023(VIII-I).31

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? T*elecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Gunay, S., & Kaskaloglu, K. (2022). Does utilizing smart contracts induce a financial connectedness between Ethereum and non-fungible tokens? *Research in International Business and Finance*, *63*, 101773. https://doi.org/10.1016/j.ribaf.2022.101773

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Hoekstra, J. (2021). Political barriers in the ratification of international commercial law conventions. *Uniform Law Review*, *26*(1), 43–66. https://doi.org/10.1093/ulr/unab003

Hughes, E., Graham, L., Rowley, L., & Lowe, R. (2018, July 1). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. *The Journal of The British Blockchain Association*, *1*(1), 63–72. https://doaj.org/article/6b966411b40746de873b99f25546bfca

Ji, B., Zhang, M., Xing, L., Li, X., Li, Ch., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digital Communications and Networks*, *9*(1), 47–55. https://doi.org/10.1016/j.dcan.2022.06.012

Kim, N. (2023). National ID for public purpose. *Georgetown Law Technology Review*, *7*(2). https://clck.ru/36kzR3

Kirli, D., Couraud, B., Robu, V., & Salgado-Bravo, M. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Liu, L., Wei-Tek, T., Zakirulm A., Hao, P., & Mingsheng, L. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. https://doi.org/10.1016/j.future.2021.08.023

Liu, H., Fan, Y., Feng, L., & Wei, Z. (2023). Vulnerable smart contract function locating based on Multi-Relational Nested Graph Convolutional Network. *Journal of Systems and Software*, *204*, 111775. https://doi.org/10.1016/j.jss.2023.111775

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://dx.doi.org/10.2139/ssrn.3440802

Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Perez, A. J., & Zeadally, S. (2023). Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review*, *43*, 100450. https://doi.org/10.1016/j.cosrev.2021.100450

Pishdad-Bozorgi, P., & Han Yoon, J. (2022). Transformational approach to subcontractor selection using blockchain-enabled smart contract as trust-enhancing technology. *Automation in Construction*, *142*, 104538. https://doi.org/10.1016/j.autcon.2022.104538

Sathiyamurthy, K., & Kodavali, L. (2023). Bayesian network-based quality assessment of blockchain smart contracts. In *Advances in Computers*. Elsevier. https://doi.org/10.1016/bs.adcom.2023.07.004

Vatiero, M. (2023). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Wang, Y., Chen, X., Huang, Y., & Hao-Nan, Z. (2023a). An empirical study on real bug fixes from solidity smart contract projects. *Journal of Systems and Software*, *204*, 111787. https://doi.org/10.1016/j.jss.2023.111787

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Xu, M. (2023b). Temporal transaction information-aware Ponzi scheme detection for ethereum smart contracts. *Engineering Applications of Artificial Intelligence*, *126*, Part C, 107022. https://doi.org/10.1016/j.engappai.2023.107022

Zhang, T., Feng, T., & Ming-li, C. (2023). Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. *Journal of Cleaner Production*, *397*, 136509. https://doi.org/10.1016/j.jclepro.2023.136509

Сведения об авторе

Ламаппулаге Донн Тарика Дишани – магистр права, магистр наук, Гринвичский университет
Адрес: Великобритания, г. Лондон, Парк Роу, SE10 9LS, Старый Королевский военно-морской колледж
E-mail: tharikadishani@gmail.com
ORCID ID: https://orcid.org/0009-0004-6820-8788
Google Scholar ID: https://scholar.google.com/citations?user=zc0kRegAAAAJ

Конфликт интересов

Автор сообщает 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: 10.89.27 / Обязательственное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 27 июля 2023 г.
Дата одобрения после рецензирования – 19 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.45

Smart Contracts and International Trade: European Legal Strategies for Managing Challenges

Tharika Dishani Lamappulage Donn

University of Greenwich
London, United Kingdom

Keywords

algorithmic code,
blockchain technology,
computer software,
digital agreement,
digital technologies,
digitalization,
electronic form,
international trade,
law,
smart contract

Abstract

Objective: the automation inherent in smart contracts makes them an attractive tool for global trade applications, especially for the automation of transactions. The prospects foreseeable will significantly impact international economic relations and the transformation of international trade rules. This fact determines the study objective – to identify the possibilities of transforming the said rules and the political and legal strategies adopted by European countries to implement smart contracts in international trade.

Methods: the study, devoted to the current international trade regulation in the context of contracts digitalization and spread of smart contracts, uses a combination of formal-legal and comparative-legal methods. They allow researching the international trade rules, analyzing and comparing the UK and the EU political and legal positions on the smart contracts introduction in international trade, as well as predicting the legal consequences of using smart contracts in international trade.

Results: the research shows that the proliferation of smart contracts has significant implications for international trade and its regulation. Smart contracts have numerous advantages, such as increased efficiency, reduced costs, and wide availability. However, they may lead to legal challenges when harmonizing traditional legal principles with the digital

environment, in particular concerning the authentication of subjects, enforceability under specific circumstances of a case, and jurisdictional issues.

Scientific novelty: the current literature on the transformation of international trade regulation in the context of digitalization processes and the spread of smart contracts is complemented by the results of a comparative analysis of the legal positions existing in the European legal space and developed on the basis of problems, lessons and achievements in the smart contracts implementation in international trade.

Practical significance: understanding the legal implications of smart contracts is important for businesses involved in international trade. The study provides insights into the UK and the EU legal positions from which guidance can be provided to companies navigating the digital landscape. Policymakers can also benefit from the findings when developing appropriate legal acts to balance the benefits of smart contracts with the need for legal certainty and protection in international trade.

For citation

Lamappulage Donn, T. D. (2023). Smart Contracts and International Trade: European Legal Strategies for Managing Challenges. *Journal of Digital Technologies and Law, 1*(4), 1042–1057. https://doi.org/10.21202/jdtl.2023.45

References

Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. *Telematics and Informatics*, *57*, 101519. https://doi.org/10.1016/j.tele.2020.101519

Bandara, E., Ng, W. K., Ranasinghe, N., & De Zoysa, K. (2019). Aplos: Smart Contracts made smart. In J. F. Ashish, Gh. R. Oliveira, P. L. Zhou (Eds.), *Communications in Computer and Information Science* (pp. 431–445). https://doi.org/10.1007/978-981-15-2777-7_35

Blaszczyk, M. (2023). *Smart contracts, Lex cryptographia, and transnational contract theory*. SSRN. https://doi.org/10.2139/ssrn.4319654

Buigut, S., & Kapar, B. (2023). How did Brexit impact EU trade? Evidence from real data. *The World Economy*, *46*(6), 1566–1581. https://doi.org/10.1111/twec.13419

Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. *Digital Society*, *2*(1). https://doi.org/10.1007/s44206-023-00038-2

Chu, H., Zhang, P., Dong, H., Xiao, Y., Shunhui, J., & Wenrui, L. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. *Information and Software Technology*, *159*(107221). https://doi.org/10.1016/j.infsof.2023.107221

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in Consumer Contracts: Machines as servants, not masters. *The Modern Law Review*. https://doi.org/10.1111/1468-2230.12817

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. (2019). Creating markets in no-trust environments: The law and economics of smart contracts. *Computer Law & Security Review*, *35*(1), 69–88. https://doi.org/10.1016/j.clsr.2018.09.003

Fatima, S. (2023). Employability of a Research Method and Methodology in a Socio-Legal Study. *Global Social Sciences Review*, *VIII*(I), 341–351. https://doi.org/10.31703/gssr.2023(VIII-I).31

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution?. T*elecommunications Policy*, *45*(2), 102081. https://doi.org/10.1016/j.telpol.2020.102081

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Gunay, S., & Kaskaloglu, K. (2022). Does utilizing smart contracts induce a financial connectedness between Ethereum and non-fungible tokens?. *Research in International Business and Finance*, *63*, 101773. https://doi.org/10.1016/j.ribaf.2022.101773

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. *Journal of Network and Computer Applications*, *177*, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Hoekstra, J. (2021). Political barriers in the ratification of international commercial law conventions. *Uniform Law Review*, *26*(1), 43–66. https://doi.org/10.1093/ulr/unab003

Hughes, E., Graham, L., Rowley, L., & Lowe, R. (2018, July 1). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. *The Journal of The British Blockchain Association*, *1*(1), 63–72. https://doaj.org/article/6b966411b40746de873b99f25546bfca

Ji, B., Zhang, M., Xing, L., Li, X., Li, Ch., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. *Digital Communications and Networks*, *9*(1), 47–55. https://doi.org/10.1016/j.dcan.2022.06.012

Kim, N. (2023). National ID for public purpose. *Georgetown Law Technology Review*, *7*(2). https://clck.ru/36kzR3

Kirli, D., Couraud, B., Robu, V., & Salgado-Bravo, M. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *158*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Liu, L., Wei-Tek, T., Zakirulm A., Hao, P., & Mingsheng, L. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. https://doi.org/10.1016/j.future.2021.08.023

Liu, H., Fan, Y., Feng, L., & Wei, Z. (2023). Vulnerable smart contract function locating based on Multi-Relational Nested Graph Convolutional Network. *Journal of Systems and Software*, *204*, 111775. https://doi.org/10.1016/j.jss.2023.111775

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. http://dx.doi.org/10.2139/ssrn.3440802

Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Papadouli, V., & Papakonstantinou, V. (2023). A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs. *Computer Law & Security Review*, *51*, 105869. https://doi.org/10.1016/j.clsr.2023.105869

Perez, A. J., & Zeadally, S. (2023). Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions. *Computer Science Review*, *43*, 100450. https://doi.org/10.1016/j.cosrev.2021.100450

Pishdad-Bozorgi, P., & Han Yoon, J. (2022). Transformational approach to subcontractor selection using blockchain-enabled smart contract as trust-enhancing technology. *Automation in Construction*, *142*, 104538. https://doi.org/10.1016/j.autcon.2022.104538

Sathiyamurthy, K., & Kodavali, L. (2023). Bayesian network-based quality assessment of blockchain smart contracts. In *Advances in Computers*. Elsevier. https://doi.org/10.1016/bs.adcom.2023.07.004

Vatiero, M. (2023). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. *Computer Law & Security Review*, *46*, 105710. https://doi.org/10.1016/j.clsr.2022.105710

Wang, Y., Chen, X., Huang, Y., & Hao-Nan, Z. (2023a). An empirical study on real bug fixes from solidity smart contract projects. *Journal of Systems and Software*, *204*, 111787. https://doi.org/10.1016/j.jss.2023.111787

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Xu, M. (2023b). Temporal transaction information-aware Ponzi scheme detection for ethereum smart contracts. *Engineering Applications of Artificial Intelligence*, *126*, Part C, 107022. https://doi.org/10.1016/j.engappai.2023.107022

Zhang, T., Feng, T., & Ming-li, C. (2023). Smart contract design and process optimization of carbon trading based on blockchain: The case of China's electric power sector. *Journal of Cleaner Production*, *397*, 136509. https://doi.org/10.1016/j.jclepro.2023.136509

Author information

Tharika Dishani Lamappulage Donn – MSc, Master Student, University of Greenwich
Address: Old Royal Naval College, Park Row, London SE10 9LS, United Kingdom
E-mail: tharikadishani@gmail.com
ORCID ID: https://orcid.org/0009-0004-6820-8788
Google Scholar ID: https://scholar.google.com/citations?user=zc0kRegAAAAJ

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 27, 2023
Date of approval – October 19, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:347.45/.47
EDN: https://elibrary.ru/lbzqze
DOI: https://doi.org/10.21202/jdtl.2023.46

Дистанционные способы совершения сделок с использованием цифровых технологий

Татьяна Александровна Савельева

Новосибирский юридический институт (филиал) Томского государственного университета
г. Новосибирск, Российская Федерация

Ключевые слова

баланс интересов,
блокчейн,
дистанционная сделка,
дистанционный договор,
информационные технологии,
искусственный интеллект,
право,
смарт-контракт,
цифровые технологии,
электронный документ

Аннотация

Цель: обоснование необходимости выделения новых договорных конструкций (моделей) с учетом специфики отношений, связанных с использованием дистанционного способа заключения договора посредством цифровых технологий и возможными рисками для их участников.

Методы: наряду со специально-юридическими методами основополагающим в процессе исследования стал метод критического анализа, что позволило оценить и интерпретировать основные источники и нормы гражданского права применительно к совершению дистанционных сделок, проанализировать современное состояние законодательства в этой области в контексте развивающихся процессов цифровизации и технологизации гражданско-правовых отношений.

Результаты: представлен критический анализ текущего состояния правовой регламентации дистанционных способов заключения договоров, дана их классификация. Сделан вывод о том, что развитие цифровых технологий порождает новые дистанционные способы совершения сделок, а также наполняет новым содержанием традиционные для гражданского права процедуры заключения договора. Обоснована целесообразность выделения понятия «дистанционная сделка» в качестве правовой категории в целях создания специального гражданско-правового режима, при этом базовым понятием должно являться понятие «дистанционный договор». Проанализированы отдельные виды дистанционных договоров для обоснования идеи о необходимости специальных правовых режимов в случаях, когда дистанционный способ заключения договора сочетается с использованием цифровых технологий, применение которых ставит такие проблемы, как распределение рисков технологических сбоев, хакерских атак, соблюдение баланса интересов сторон с учетом информационной асимметрии, необходимость защиты слабой стороны.

Научная новизна: предпринята попытка дать определение таких понятий, как «дистанционный договор», «дистанционная сделка», выделить их признаки. Обоснована целесообразность рассмотрения дистанционного договора в качестве самостоятельной правовой конструкции (модели) договора, в рамках которой должен быть разработан и закреплен специальный правовой режим, который может быть распространен на односторонние дистанционные сделки. Сформулированы проблемы правового регулирования, обусловленные использованием информационных технологий, а также предложены правовые конструкции для их решения.

Практическая значимость: сделанные выводы и предложения могут быть использованы как в договорной практике участниками гражданского оборота, так и для нормативного закрепления понятия и признаков «дистанционного договора», «дистанционной сделки», создания специального правового режима с учетом специфики, порождаемой использованием цифровых технологий.

Для цитирования

Савельева, Т. А. (2023). Дистанционные способы совершения сделок с использованием цифровых технологий. *Journal of Digital Technologies and Law*, *1*(4), 1058–1086. https://doi.org/10.21202/jdtl.2023.46

Содержание

Введение

Развитие цифровых технологий затрагивает все сферы деятельности человека, включая взаимоотношения участников гражданского оборота при совершении и исполнении сделок.

Цифровые технологии позволяют участникам гражданского оборота вести переговоры, вступать в договорные отношения, обмениваться документами, осуществлять и принимать исполнение, доводить свое волеизъявление до другой стороны дистанционно. При этом использование цифровых технологий делает дистанционное взаимодействие сторон по договору принципиально иным по сравнению с периодом «доцифровой» эпохи.

Действующее законодательство пытается учесть развитие информационных технологий. Так, Гражданский кодекс Российской Федерации (далее – ГК РФ или Кодекс)[1] был дополнен в 2019 г. нормами, предусматривающими возможность заключения договора в электронной форме (путем обмена электронными сообщениями, путем заключения одного электронного документа)[2].

Между тем законодатель не выделяет дистанционные сделки в качестве отдельной категории. Возникает закономерный вопрос о целесообразности такого выделения с точки зрения практических потребностей гражданского оборота, а также с точки зрения доктрины. Достаточно ли того, что в законе предусмотрена электронная форма сделки?

Критерием правильности ответа на этот вопрос должен быть тест относительно соблюдения баланса интересов сторон по сделкам, заключаемым дистанционно. Достигается ли он в рамках текущей правовой регламентации, когда отсутствует специальный правовой режим, обусловленный дистанционным характером взаимодействия сторон, исключающим непосредственное восприятие волеизъявления другой стороны, ознакомление с предметом сделки в момент ее совершения и т. п.?

Следует отметить, что большое количество юридической литературы посвящено исследованию электронной формы сделки, при этом ряд важных аспектов, касающихся дистанционного взаимодействия сторон и выходящих за пределы формы сделки, остаются без должного внимания, включая вопрос о соблюдении баланса интересов сторон.

Между тем очевидно, что оценка эффективности процесса цифровизации дистанционных способов совершения сделок должна осуществляться через призму соблюдения баланса интересов сторон. В противном случае не будут достигнуты ни цели цифровизации, ни цели правового регулирования.

Следует отметить, что заключение договора путем обмена сообщениями, письмами, равно как и путем подписания одного документа, являются традиционными для гражданского права и достаточно детально урегулированы в ГК РФ.

Возможность обмена электронными сообщениями с использованием цифровых технологий, на первый взгляд, не меняет сути традиционного подхода, поскольку меняется только форма сообщения. То же самое можно сказать и по поводу возможности заключения договора путем подписания одного электронного документа.

---

1 Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (с изменениями). СПС «Консультант Плюс». https://clck.ru/36brfs

2 О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации. № 34-ФЗ от 18.03.2019. (2019). Собрание законодательства РФ, 12, ст. 12.

Однако такой взгляд является поверхностным. Ведь использование цифровых технологий с неизбежностью порождает риски технологического характера, включая риски уничтожения или искажения содержания электронного документа, риски нарушения интересов одной из сторон в силу возможной информационной асимметрии и т. п.

Настоящее исследование посвящено анализу дистанционных способов совершения сделок с использованием цифровых технологий, с тем чтобы оценить, насколько традиционные подходы к заключению гражданско-правового договора и состояние действующего гражданско-правового законодательства соответствуют новым вызовам, которые возникают в связи с активным использованием цифровых технологий в сфере взаимодействия участников договорных отношений.

Работа состоит их трех частей. В первой части будут проанализированы дистанционные способы заключения договора и совершения односторонних сделок, их особенности, связанные с использованием цифровых технологий, с тем чтобы сделать вывод о наличии или отсутствии целесообразности выделения «дистанционного договора» и «дистанционной сделки» в качестве правовых понятий. Вторая часть работы посвящена рассмотрению отдельных видов дистанционных договоров в аспекте соблюдения баланса интересов сторон. В третьей части будут рассмотрены аспекты, касающиеся дистанционного взаимодействия сторон, которые выходят за рамки частноправового регулирования, но могут служить подтверждением или опровержением целесообразности рассмотрения дистанционных сделок в качестве правового понятия с установлением специального правового режима.

1. Понятие и виды дистанционных сделок

1.1. Сфера использования и регламентация дистанционного способа заключения гражданско-правового договора

В гражданском обороте широкое распространение получил дистанционный способ заключения различных сделок. В нашу жизнь прочно вошли дистанционная торговля, дистанционное банковское обслуживание, включая расчеты с использованием банковских карт, кредитование и даже заключение сделок с недвижимостью в дистанционном формате. К дистанционному способу совершения сделок можно отнести любые сделки, когда стороны вместо физического присутствия на этапе переговоров и совершения сделки используют средства дистанционной связи, включая почтовые сообщения, электронную почту, СМС-сообщения, Интернет и др.

Что касается правового регулирования дистанционного способа заключения сделок, то здесь следует отметить отсутствие системного подхода, который учитывал бы специфику отношений, связанных с использованием данного способа заключения договора применительно к различным сферам. Так, дистанционный способ розничной продажи товаров достаточно детально урегулирован законодательством[3].

[3] Гражданский кодекс Российской Федерации (часть вторая) № 14-ФЗ от 26.01.1996 (ред. от 24.07.2023) (с изм. и доп., вступ. в силу с 12.09.2023), ст. 497. СПС «Консультант Плюс». https://clck.ru/36briF ; О защите прав потребителей. № 2300-1 от 07.02.1992 (с изменениями), ст. 26.1. СПС «Консультант Плюс». https://clck.ru/36brjV ; Постановление Правительства Российской Федерации № 2463 от 31.12.2020. (2020). СПС «Консультант Плюс». https://clck.ru/36brka

Говоря об иных сферах использования дистанционного способа заключения договоров, следует отметить отсутствие специального правового регулирования, за редкими исключениями, которые будут рассмотрены далее. Такой подход вызван тем, что законодатель, вероятно, исходит из отсутствия такой необходимости регламентации.

С учетом указанного представляется важным проанализировать действующие правовые нормы общего характера, касающиеся дистанционного способа заключения договоров, для того чтобы оценить достаточность правовой регламентации с учетом стремительного развития цифровых технологий и их использования на практике. Процесс цифровизации требует переосмысления многих традиционных взглядов на договорную сферу, включая дистанционный способ заключения договора. При анализе мы оставляем за рамками вопросы использования искусственного интеллекта в области взаимодействия участников гражданско-правовых договоров.

При этом нельзя не признать увеличение влияния искусственного интеллекта на все сферы нашей жизни, одним из проявлений такого влияния является перенос коммуникаций в виртуальную среду (киберпространство) (Филипова, 2023). С учетом указанного тема влияния искусственного интеллекта на процесс взаимодействия сторон при дистанционном способе заключения сделок заслуживает отдельного исследования.

В силу п. 1 ст. 160 ГК РФ сделка в письменной форме должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, либо должным образом уполномоченными ими лицами. Письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Законом, иными правовыми актами и соглашением сторон может быть предусмотрен специальный способ достоверного определения лица, выразившего волю.

Любой договор, заключаемый между отсутствующими, может быть квалифицирован в качестве дистанционной сделки в широком смысле слова.

В Кодексе детально урегулирован порядок заключения договора именно между отсутствующими, который включает направление предложения (оферты), ее рассмотрение акцептантом, направление им акцепта, его получение оферентом. В силу п. 1 ст. 433 ГК РФ «договор признается заключенным в момент получения лицом, направившим оферту, ее акцепта»[4].

Законодателем установлены последствия направления оферты, содержащей срок для акцепта (ст. 440 ГК РФ), оферты, не содержащей срока для акцепта (ст. 441 ГК РФ), последствия опоздания акцепта (ст. 443 ГК РФ) и т. п.

К дистанционному способу заключения договора можно отнести и заключение договора путем совершения акцептантом конклюдентных действий. Так, в силу п. 3 ст. 438 ГК РФ совершение лицом, получившим оферту, в срок, установленный для ее

[4] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 24.07.2023) (с изм. и доп., вступ. в силу с 01.10.2023). СПС «КонсультантПлюс». https://clck.ru/36eEQ9

акцепта, действий по выполнению указанных в ней условий договора (отгрузку товаров, предоставление услуг, выполнение работ, уплату соответствующей суммы и т. п.) считается акцептом, если иное не предусмотрено законом, иными правовыми актами или не указано в оферте.

Развитие цифровизации, возможность направления оферты и акцепта путем применения информационных технологий делают необходимым по-новому взглянуть на порядок заключения договора между отсутствующими, выделить в отдельную категорию договоры, заключаемые дистанционно путем обмена документами не в традиционной бумажной форме.

Кроме того, сфера использования дистанционного способа заключения договора охватывает не только заключение договора путем обмена письмами, сообщениями по типу оферта – акцепт, но и путем подписания одного документа в электронной форме.

В 2019 г. в Кодекс внесены важные изменения, в частности в ст. 434 ГК РФ. В силу п. 2 данной статьи договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными в соответствии с правилами абзаца второго п. 1 ст. 160 Кодекса.

Как известно, путем подписания одного документа подлежат заключению договоры по поводу недвижимого имущества (ст. 550, 560, 651, 658 ГК РФ), корпоративный договор (ст. 67.2 ГК РФ), договор о создании акционерного общества (ст. 98 ГК РФ) и др. Договоры, заключаемые путем подписания одного электронного документа, безусловно, могут быть отнесены к дистанционным договорам.

Ряд договоров, заключаемых путем одного документа, требуют нотариального удостоверения. В частности, нотариальному удостоверению подлежат договор ренты (ст. 584 ГК РФ), сделка, направленная на отчуждение доли в уставном капитале общества с ограниченной ответственностью (п. 11 ст. 21 Закона об обществах с ограниченной ответственностью)[5].

Участники гражданского оборота могут нотариально удостоверить сделки в случаях, предусмотренных соглашением сторон, хотя бы по закону для сделок данного вида эта форма не требовалась (п. 2 ст. 163 ГК РФ). В рамках процесса цифровизации в нашей стране нотариат в 2019 г. был наделен полномочиями по совершению нотариальных действий в дистанционном режиме. Одной из новелл явилось включение правил об удостоверении сделки с участием двух и более нотариусов без их личного присутствия[6].

Речь идет о ситуации, когда стороны сделки находятся в разных регионах и совершают сделку, не покидая место своего нахождения. При этом нотариальное удостоверение сделки осуществляется нотариусами разных регионов. Стороны сделки с участием нотариусов готовят проект договора, затем подписывают текст на

---

5 Об обществах с ограниченной ответственностью. № 14-ФЗ от 08.02.1998 (ред. от 13.06.2023). СПС «Консультант Плюс». https://clck.ru/36brni

6 О внесении изменений в Основы законодательства Российской Федерации о нотариате и отдельные законодательные акты Российской Федерации. № 480-ФЗ от 27.12.2019. (2019). Собрание законодательства РФ, 52 (ч. I), ст. 7798.

бумажном носителе и в электронном варианте. Такие договоры также могут быть отнесены к дистанционным сделкам.

Важную категорию дистанционных сделок составляют смарт-контракты. Смарт-контракты могут использоваться в различных сферах и на разных стадиях договорных отношений. Они позволяют потребителям выбирать поставщика, вступать с ним в договорные отношения. При развертывании на блокчейне смарт-контракты могут автоматически заключать соглашения и обеспечивать их соблюдение (Kirli et al., 2022).

Сразу отметим, что законодательное определение смарт-контракта отсутствует. В литературе высказаны разные точки зрения относительно их правовой природы. Юридическая общественность пытается найти ответы на вопрос о возможности применить к смарт-контракту в той или иной мере традиционные договорные конструкции (Савельев, 2016; Белов, 2021; Ефимова, 2019; Чурилов, 2020; Шелепина, 2021; Цепов, Иванов, 2022; Челышева, 2022; Hsain et al., 2021).

Между тем, несмотря на споры относительно понятия смарт-контракта, как справедливо отмечается в литературе, смарт-контракты реально используются в повседневной жизни, например при вызове такси, аренде автомобилей и др. (Уткин, 2022).

По мнению ряда авторов, «смарт-контрактом называется компьютерная программа (или компьютерный код), которая может быть заключена только с использованием технологии blockchain и позволяет автоматически заключать, исполнять и прекращать различные договоры по наступлении заранее установленных юридических фактов» (Ефимова, Сиземова, 2019).

В проекте федерального закона «О цифровых финансовых активах» было дано такое определение: «Смарт-контракт – договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределенном реестре цифровых транзакций в строго определенной таким договором последовательности и при наступлении определенных им обстоятельств»[7].

Данное определение было исключено из текста закона, а в ходе обсуждения законопроекта с отрицательным мнением по этому вопросу выступил Комитет по экономической политике, промышленности, инновационному развитию и предпринимательству, который указал, что «смарт-контракт по сути есть компьютерный алгоритм, позволяющий участникам распределенного реестра обмениваться активами, представляет собой технологию и не может признаваться видом гражданско-правового договора». В заключении данного Комитета было указано, что по смарт-контрактам в ст. 309 ГК РФ вводится единственное и достаточное для регулирования правило: «факт совершенного компьютерной программой исполнения сделки не оспаривается (кроме случаев вмешательства в действие программы). После идентификации пользователей в системе дальнейшее их поведение подчиняется алгоритму компьютерной программы, организующей сеть, а лицо, «покупающее» тот или иной виртуальный объект (цифровое право), получит этот объект автоматически»[8].

---

7 О цифровых финансовых активах: проект федерального закона № 419059-7 (ред., внесенная в ГД ФС РФ, текст по состоянию на 20.03.2018). СПС «Консультант Плюс». https://clck.ru/36bron

8 Заключение Комитета по экономической политике, промышленности, инновационному развитию и предпринимательству от 03.04.2018 № 3.8/522 «По проекту федерального закона № 419059-7 «О цифровых финансовых активах». СПС «Консультант Плюс». https://clck.ru/36brpn

Исследователи справедливо отмечают, что одной из наиболее актуальных проблем при использовании смарт-контрактов является то, что они основаны на процедурных языках программирования. Код, изложенный на процедурном языке, обычно должен указывать, как решить проблему, явно предоставляя четкие инструкции, которые управляют его поведением (Ferro et al., 2023).

Вопросы, касающиеся смарт-контрактов, требуют отдельного исследования в силу объемности материала, неоднозначности ряда исходных позиций как в понимании смарт-контракта, так и в понимании надежности получаемых результатов при использовании смарт-контракта с учетом того, что они также подвержены атакам (Aquilina et al., 2021).

В настоящей работе рассмотрение смарт-контракта будет затронуто лишь в той мере, в какой это будет необходимым для анализа дистанционных сделок как правовой категории в целом. Говоря о правовой регламентации порядка совершения дистанционных сделок, следует отметить, что обеспечение конфиденциальности информации, включая персональную информацию, является отдельным актуальным аспектом совершения сделок в дистанционном формате.

Особую актуальность этот вопрос приобретает при совершении сделок с иностранным элементом, когда имеет место экспорт личной информации. Неслучайно администрация киберпространства Китая («CAC») 24 февраля 2023 г. выпустила «Меры по стандартным контрактам на экспорт личной информации» (Kennedy, 2023).

Представляется, что вопросы экспорта персональных данных в рамках дистанционных сделок с иностранным элементом требуют отдельного исследования, с тем чтобы на законодательном уровне закрепить механизмы по контролю передачи таких данных за пределы Российской Федерации.

В продолжение темы правовой регламентации использования цифровых технологий при дистанционном взаимодействии участников сделки необходимо обозначить еще один аспект, выходящий не только за рамки гражданско-правового регулирования, но и, возможно, за рамки правового регулирования вообще. Речь идет о различиях в правосознании юристов, которые занимаются правотворческой и правоприменительной деятельностью, и субъектов, которые осуществляют технические разработки использования цифровой среды в различных сферах жизни человека, включая дистанционное взаимодействие. Интересное исследование в этой сфере проведено зарубежными авторами, которыми выявлено принципиально разное понимание безопасности у юристов и робототехников (Rompaey et al., 2022).

Рассмотрение данного вопроса выходит за пределы настоящей работы, вместе с тем мы не можем не отметить эту проблему в качестве одной из возможных причин тех затруднений, с которыми сталкивается внедрение новых технических достижений в сферу юриспруденции.

Подытоживая изложенное, можно констатировать, что дистанционный способ заключения договора, т. е. без одновременного личного присутствия сторон и выражения воли в месте заключения договора, не является новым для законодательства. Правовая регламентация порядка заключения договора «между отсутствующими» всегда являлась достаточно детальной. Вместе с тем развитие цифровых технологий порождает новые дистанционные способы заключения договоров, наполняет ранее установленные процедуры взаимодействия сторон новым содержанием.

1.2. О понятии дистанционной сделки. Виды дистанционных договоров и иных сделок

Действующее законодательство не выделяет дистанционные сделки в отдельную категорию, не устанавливает специального правового режима для их участников, ограничившись регламентацией электронной формы сделки.

Как было указано ранее, дистанционный способ заключения договора не является чем-то новым для нашего законодательства. Обмен письменными сообщениями является классическим способом заключения договора. Вместе с тем нельзя не признать, что дистанционный способ взаимодействия участников сделки порождает определенную специфику во взаимоотношениях. Ведь данный способ исключает непосредственное ознакомление стороны сделки с ее предметом на этапе выражения воли, ограничивает возможности по идентификации участника сделки, а также непосредственное восприятие воли другой стороны. Накладываемое на эту специфику применение цифровых технологий существенным образом влияет на процесс взаимодействия сторон, неизбежно порождает риски, обусловленные использованием данных технологий.

Все это позволяет поставить вопрос о целесообразности выделения понятия дистанционной сделки в качестве правовой категории, а также о необходимости создания специального правового режима с учетом обеспечения баланса интересов сторон сделки. Ведь дистанционное взаимодействие с использованием цифровых технологий порождает вопросы, связанные с информационной асимметрией, необходимостью признания участника сделки слабой стороной и предоставления ей адекватных способов защиты, распределения рисков технологического характера и т. п.

Ранее мы рассмотрели вопросы, связанные с правовой регламентацией дистанционных способов заключения гражданско-правовых договоров, среди которых можно выделить:

1) договоры, заключаемые при дистанционном способе продажи товаров в розницу;

2) договоры, заключаемые путем обмена письменными сообщениями в классической форме;

3) договоры, заключаемые путем обмена электронными сообщениями;

4) договоры, заключаемые путем совершения конклюдентных действий;

5) договоры, заключаемые дистанционно путем подписания одного документа в электронной форме;

6) договоры, заключаемые дистанционно в нотариальной форме (путем удостоверения двумя или несколькими нотариусами);

7) смарт-контракты.

Возникает вопрос, можно ли считать все эти договоры дистанционными. Для ответа на этот вопрос необходимо определиться с самим понятием дистанционного договора.

Если под дистанционным договором понимать любой договор, который заключен без личного присутствия сторон в момент выражения воли в месте заключения договора, то практически все перечисленные договоры можно считать дистанционными.

Представляется, что такое понимание дистанционного договора было бы излишне широким, поскольку не отвечало бы целям создания специального правового режима данного вида договора.

Специальный правовой режим, на наш взгляд, требуется там, где дистанционный способ заключения договора сочетается с использованием цифровых технологий. Именно применение цифровых технологий ставит такие проблемы, как распределение рисков технологических сбоев, хакерских атак, соблюдения баланса интересов сторон, защиты слабой стороны, которые должны быть решены в рамках специального правового режима.

Если свести дистанционный порядок взаимодействия сторон в ходе заключения и исполнения договора только к специфике формы договора (к тому, что договор заключается в электронной форме), то все указанные выше аспекты останутся вне зоны внимания.

Вместе с тем нельзя отрицать важность вопросов, касающихся заключения договора в электронной форме. Здесь большое значение имеет овладение определенными навыками работы через интернет-сервисы, повышение правовой грамотности участников гражданского оборота, более глубокое изучение юристами особенности электронной формы договора, уяснение особенностей по сравнению с классическим договором (Tărchilă & Nagy, 2015).

Целесообразность выделения дистанционного договора в качестве самостоятельной правовой категории состоит в том, что позволяет сместить акценты с формы договора на специфику установления содержания договора, объема возникших прав и обязанностей, распределение рисков исходя из дистанционного характера взаимодействия сторон.

С этих позиций в качестве видов дистанционных договоров следует рассматривать:

1) договоры, заключаемые в сети Интернет;

2) договоры, заключаемые путем обмена электронными сообщениями;

3) договоры, заключаемые дистанционно путем подписания одного документа в электронной форме;

4) договоры, заключаемые дистанционно в нотариальной форме (путем удостоверения двумя или несколькими нотариусами);

5) смарт-контракты.

Все перечисленные виды договоров объединяет то, что стороны дистанционно взаимодействуют на преддоговорной стадии, на этапе заключения договора и, как правило, на стадии исполнения договора. Выражение воли осуществляется опосредованно, волеизъявление воспринимается другой стороной посредством информационных технологий.

При этом одна из сторон договора может являться правообладателем информационного ресурса, с помощью которого осуществляется обмен волеизъявлениями. Более того, эта сторона формирует правила дистанционного взаимодействия, в силу чего обладает информационным преимуществом в договорном процессе.

Все это требует наделения другой стороны определенными гарантиями, которые возможны в рамках специального правового режима. В рамках данного правового режима должны быть решены как минимум следующие вопросы:

– о критериях установления статуса сторон договора, признания одной из них слабой стороной;

– об условиях ответственности сторон, в том числе о применении принципа «строгой» ответственности (независимо от наличия вины), о пределах его применения;

– о том, кто несет риски технологических сбоев, хакерских атак;

– о распределении бремени доказывания между сторонами.

Представляется, что дистанционный договор должен быть выделен законодателем в качестве самостоятельной договорной конструкции, наряду с иными договорными конструкциями, содержащимися в ч. 1 ГК РФ (опционный договор, абонементный договор и др.). В качестве обоснования можно указать на то, что обладает неменьшей спецификой, а складывающиеся отношения в рамках такого договора требуют установления специального правового режима.

В последующей части настоящей работы будут рассмотрены вопросы соблюдения баланса интересов сторон применительно к отдельным видам перечисленных выше дистанционных договоров, что, как представляется, послужит дополнительным аргументом в подтверждение целесообразности выделения дистанционного договора в отдельную договорную конструкцию.

Следующий вопрос, который целесообразно затронуть, касается односторонних сделок, а именно имеет ли право на существование понятие дистанционной односторонней сделки наряду с понятием дистанционного договора. При ответе на данный вопрос необходимо исходить из существа односторонней сделки и последствий ее совершения.

В силу п. 2 ст. 154 ГК РФ односторонней считается сделка, для совершения которой в соответствии с законом, иными правовыми актами или соглашением сторон необходимо и достаточно выражения воли одной стороны. С учетом содержания ст. 160 ГК РФ односторонняя сделка может быть совершена в электронной форме.

В силу ст. 155 ГК РФ односторонняя сделка создает обязанности для лица, совершившего сделку. Она может создавать обязанности для других лиц лишь в случаях, установленных законом либо соглашением с этими лицами. Именно односторонний характер волеизъявления, отсутствие последствий в виде создания обязанностей для других лиц порождает сомнения в возможности существования дистанционных односторонних сделок.

Вместе с тем следует отметить, что односторонние сделки в ряде случаев могут быть признаны дистанционными. Так, в литературе рассматриваются перспективы дистанционного участия нотариуса в удостоверении завещаний (Яценко, 2019; Михайлова, 2020). В этом случае завещание будет являться дистанционной сделкой.

Далее необходимо учитывать еще один важный аспект. Среди односторонних сделок выделяют сделки, требующие восприятия, и сделки, не требующие восприятия (Акужинов, 2020). Относительно сделок, требующих восприятия, А. В. Егоров указывает: «Смысл выделения данной категории состоит в том, что эта разновидность односторонних сделок получает силу не с момента совершения волеизъявления, а с момента поступления данного волеизъявления адресату» (Егоров, 2015).

Следует отметить, что большинство односторонних сделок являются сделками, требующими восприятия. К ним, в частности, относится односторонний отказ от договора (исполнения договора). В силу ст. 450.1 ГК РФ право на односторонний отказ от договора (исполнения договора) может быть осуществлено управомоченной стороной путем уведомления другой стороны об отказе от договора (исполнения договора). Договор прекращается с момента получения данного уведомления, если иное не предусмотрено настоящим Кодексом, другими законами, иными правовыми актами или договором. Какие-либо препятствия заявить об одностороннем отказе от договора в электронной форме отсутствуют (безусловно, при наличии оснований для отказа от договора во внесудебном порядке).

В данном случае мы имеем, на первый взгляд, противоречивую ситуацию. С одной стороны, реализация права на отказ от договора не зависит от контрагента, его отношение к этому и его поведение являются безразличными с точки зрения правовых последствий для лица, отказывающегося от договора. С этой точки зрения односторонний отказ от договора не должен рассматриваться в качестве дистанционной сделки.

С другой стороны, отказ от договора должен быть не только заявлен, но и воспринят контрагентом. Это означает, что, несмотря на то, что поведение контрагента является безразличным для лица, отказывающегося от договора, тем не менее совершение односторонней сделки предполагает взаимодействие с контрагентом.

В случае если такое взаимодействие будет осуществляться с использованием информационных технологий, есть все основания для того, чтобы был создан специальный правовой режим, о котором речь шла ранее. Указанное свидетельствует о том, что односторонние сделки, требующие восприятия, могут быть отнесены к дистанционным сделкам, если доведение волеизъявления до контрагента осуществляется с использованием цифровых технологий.

При этом, как представляется, базовым понятием должно являться понятие дистанционного договора. В рамках конструкции дистанционного договора должен быть разработан и закреплен специальный правовой режим, который может быть распространен на односторонние сделки.

2. Обеспечение баланса интересов сторон при совершении ряда дистанционных сделок

2.1. Договоры, совершаемые через интернет-сайты

Заключение сделок в сети Интернет получило столь широкое распространение, что делает необходимым рассмотрение порядка совершения сделок через призму соблюдения баланса интересов сторон.

Прежде всего, следует отметить, что в тех случаях, когда заключение определенных соглашений доступно исключительно благодаря участию в интернет-сервисах, это означает невозможность осуществления различных форм деятельности без доступа в Интернет (Lim & Pan, 2021) и должно рассматриваться в качестве фактора, нарушающего права потенциальных потребителей.

Данный аспект выходит за рамки частноправового регулирования и заслуживает отдельного исследования. Однако его нельзя игнорировать, когда речь идет о балансе интересов участников гражданского оборота.

Далее, рассмотрим особенности порядка заключения договоров через интернет-сайты в аспекте гражданско-правового регулирования. Любой договор представляет собой соглашение сторон, содержанием которого является совокупность условий, о которых стороны договорились. Поэтому важным является ознакомление пользователя с условиями договора (офертой, размещенной на сайте). Ведь бездумное нажатие на кнопку «согласен» грозит непредсказуемыми последствиями.

Основные варианты выражения пользователем согласия с условиями договора, размещенными на сайте, зависят от способа размещения на сайте условий соглашения, т. е. оферты.

1. Текст соглашения размещен непосредственно на странице сайта.

2. Оферта непосредственно на странице сайта не размещена, ознакомление возможно путем перехода по гиперссылке.

3. На сайте размещена запись о предполагаемом согласии пользователя с условиями в случае продолжения использования сайта.

При этом варианте вообще возникают сомнения относительно того, можно ли считать договор заключенным, и они должны разрешаться с учетом конкретных обстоятельств (Гринь, 2019).

Порядок заключения договора через интернет-сайты нарушает баланс интересов сторон. Пользователь в силу информационного неравенства является слабой стороной и должен наделяться соответствующими способами защиты, к числу которых можно отнести предусмотренное п. 2 ст. 428 ГК право стороны договора потребовать изменения или расторжения договора с ретроспективным эффектом.

Подытоживая краткое рассмотрение вопроса о заключении договоров через интернет-сайты, следует констатировать, что договоры, заключаемые через интернет-сайты, соответствуют условиям, являющимся основанием для квалификации таких договоров в качестве договоров присоединения в силу ст. 428 ГК РФ.

Способом соблюдения баланса интересов сторон являлось бы закрепление правила о распространении на сделки, совершаемые через интернет-сайты, режима договора присоединения. При этом владельцу сайта могла бы быть предоставлена возможность исключить действие ст. 428 ГК РФ в случае, когда на сайте будет техническая возможность для потребителя участвовать ему в выработке, корректировке условий соглашения, размещенных на сайте.

При этом заслуживает поддержки мнение о том, что «механизмы защиты, которые заложены в п. 3 ст. 428 ГК РФ, не могут быть реализованы в полной мере. Речь идет об отсутствии в законодательстве определенных критериев, позволяющих на практике «расшифровать» (или конкретизировать), имеются ли в правоотношениях неравенство переговорных возможностей и определение условий договора только одной из сторон, которые дают слабой стороне названные правовые гарантии» (Овчинникова, 2022).

Следует согласиться с высказанным в литературе мнением о том, «действующее регулирование не позволяет в должной мере оценить добросовестность и равенство участников соглашения, если условия сформированы только одной стороной с использованием компьютерных технологий» (Кузьмина, Ломакина, 2022).

Таким образом, изложенное позволяет прийти к выводу, что порядок заключения договоров через интернет-сайты нарушает баланс интересов сторон. Пользователь является слабой стороной в силу информационной асимметрии, неравенства переговорных возможностей, что требует установления специального правового режима в рамках регулирования отношений сторон по порядку совершения таких сделок.

Кроме того, требует отдельного исследования вопрос о целесообразности законодательного ограничения случаев, когда отсутствие доступности интернет-сервисов исключает возможность заключения договоров и влечет ограничение доступа к товарам, услугам или является препятствием для осуществления определенных видов деятельности.

2.2. Договоры, заключаемые путем составления одного электронного документа, подписанного сторонами

В п. 2 ст. 434 ГК РФ предусмотрено, что договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами. Подписание договоров осуществляется электронными подписями[9]. Такой договор в полной мере может быть отнесен к дистанционному договору.

В литературе высказывается сомнение относительно того, что возможность использования электронной формы договора в виде одного документа появилась только после внесения изменений в Кодекс в 2019 г. (Костикова, 2022). Использование данного способа заключения договора стало достаточно распространенной практикой в сфере недвижимости. Так оформляются договоры купли-продажи, договоры долевого участия в строительстве объектов недвижимого имущества, акты приема-передачи недвижимого имущества.

Детальный анализ сделок с недвижимым имуществом выходит за рамки настоящего исследования. Вместе с тем хотелось бы выразить свое отношение к оформлению в дистанционном режиме документов о передаче недвижимого имущества. Представляется, что допущение такого способа оформления актов применительно к недвижимости со стороны законодателя было поспешным, недостаточно проработанным. При этом «риски возникают у обеих сторон. Покупатель может столкнуться с тем, что состояние недвижимости не соответствует тому, как оно было показано продавцом дистанционно путем видеосвязи. Процесс доказывания для покупателя будет осложнен, поскольку результаты показа не зафиксированы. Кроме того, покупатель в данном случае, подписав акт приема-передачи, фактически не получает владение недвижимостью.

Для продавца такое оформление сделки и акта приема-передачи также может создать проблемы. Так, недобросовестный покупатель получает возможность ставить вопрос о том, что он заключил сделку под влиянием обмана или заблуждения, поскольку не осматривал объект недвижимости. Кроме того, покупатель может также ставить вопрос о том, что фактической передачи недвижимости не было, подписание акта носило фиктивный характер» (Савельева, 2022).

Изложенное свидетельствует о наличии нерешенных вопросов в связи с дистанционным характером взаимодействия сторон.

2.3. Договоры, заключаемые дистанционно в нотариальной форме (путем удостоверения двумя или несколькими нотариусами)

Необходимость и эффективность внедрения в нотариальную деятельность цифровых технологий не вызывает сомнений. Дистанционный порядок нотариального удостоверения сделок существенно упрощает получение нотариальных услуг участниками гражданского оборота.

Стороны сделки, находящиеся в разных регионах, могут заключить договор и удостоверить его нотариально, не покидая свое место нахождения.

---

[9] Об электронной подписи. № 63-ФЗ от 06.04.2011 (с изменениями и дополнениями). СПС «Консультант Плюс». https://clck.ru/36brtE

Процедура заключения таких дистанционных сделок включает следующие основные этапы:

1) предварительное согласование сторонами условий договора;

2) выбор каждым участником сделки нотариуса по месту своего нахождения;

3) оформление нотариусом паспорта сделки в программном комплексе, включая сведения о сделке, участниках, представителях;

4) добавление в базу документов;

5) фиксация информации:

– подписание стороной сделки простой электронной подписью сведений об участнике сделки,

– подписание нотариусом усиленной квалифицированной подписью сведений об участнике сделки;

6) обмен между нотариусами сведениями в базе данных, согласование паспорта сделки, последствием является блокирование всех операций с согласованной частью паспорта сделки;

7) подписание паспорта сделки всеми нотариусами;

8) удостоверение сделки, включая:

– связь в формате видеоконференции, прочтение договора сторонами (представителями),

– подписание каждой из сторон своего экземпляра договора на бумажном носителе,

– подписание каждой из сторон договора простой электронной подписью,

– подписание нотариусами договора квалифицированной электронной подписью,

– завершение видеоконференции и регистрация записи нотариусами;

9) направление документов на государственную регистрацию.

Как мы видим, договор оформляется и подписывается не только в электронной форме, но и на бумажном носителе. В связи с этим в литературе справедливо ставится вопрос об установлении момента выражения воли лица совершить сделку (Лаптев, Соловяненко, 2022).

В рассматриваемом нами аспекте применительно к данному виду дистанционных договоров следует проанализировать, насколько механизм заключения такой сделки является надежной гарантией ее участников. Необходимо отметить, что дистанционный характер удостоверения сделки не снижает уровень требований к деятельности нотариуса по обеспечению законности сделки. Как и при удостоверении сделок в очном формате, нотариус проверяет правоспособность и дееспособность, устанавливает волю и добровольность волеизъявления, разъясняет последствия сделки, проверяет законность содержания сделки.

Вместе с тем использование информационных технологий, создавая удобства и комфорт для сторон сделки, имеет своей оборотной стороной возникновение рисков безопасности сделок. К таким рискам относятся риски уничтожения или искажения содержания электронных сделок в силу хакерских атак, внедрения вируса в программу. Возможны проблемы с идентификацией при дистанционном взаимодействии.

Следует согласиться с мнением Е. А. Кирилловой, что «цифровизация российского нотариата предоставляет новые возможности для граждан, однако цифровые технологии – это лишь вспомогательный инструмент, который не сможет

заменить такого специалиста, как нотариус, гарантирующего законность совершаемых сделок» (Кириллова, 2021).

При этом возникают вопросы о последствиях технологических сбоев, в том числе о порядке установления действительной воли сторон, о порядке истребования и оценке цифровых доказательств, многие из которых, к сожалению, на текущий момент не имеют ответов.

2.4. Сделки, совершаемые посредством обмена электронными документами

При анализе дистанционных сделок в аспекте соблюдения баланса интересов сторон невозможно игнорировать договоры, заключаемые путем обмена электронными документами.

Анализ судебной практики показывает значительное количество споров, в рамках которых суд вынужден давать оценку сообщениям, направленным по электронной почте[10], СМС, переписке в мессенджерах[11] и т. п.

Следует отметить, что аналогичные вопросы рассматриваются судами зарубежных стран. В литературе отмечается, что в целом тенденция складывается в пользу признания подобной переписки в качестве допустимых доказательств, однако это не безусловное положение. В каждом конкретном деле судья оценивает допустимость такого доказательства (Козлова, Сергачева, 2022).

Представляется, что законодатель и/или, возможно, высшие судебные инстанции должны дать относительно четкие ориентиры участникам гражданского оборота по поводу возможности или невозможности использования средств дистанционных коммуникаций без электронной подписи применительно к типизированным ситуациям.

Наиболее безопасным для участников гражданского оборота является выстраивание двухступенчатой системы при использовании электронных сообщений:

– заключение соглашения об осуществлении электронного документооборота в традиционной форме (с указанием конкретных видов документов, адресов переписки);

– собственно обмен электронными документами.

Отметим, что в банковской практике широко распространено заключение подобных соглашений об электронном документообороте.

В других сферах, к сожалению, такое выстраивание электронного документооборота практически не применяется. Стороны обмениваются скан-копиями проектов договоров, протоколов разногласий, направляют письма-оферты, письма-акцепты, акты, иные документы во исполнение договорных обязательств по электронной почте. При этом никаких документов, летитимирующих электронный документооборот, сторонами не оформляется.

---

[10] Постановление Президиума ВАС РФ № 18002/2012 от 12.11.2013 по делу А47-7950/2011. СПС «Консультант Плюс». https://clck.ru/36brts

[11] Определение Пермского кассационного суда общей юрисдикции № 88-22889/2020 от 30.10.2020 по делу № 2-1314/2019; Определение Третьего кассационного суд общей юрисдикции № 88-17185/2020 от 29.10.2020. СПС «Консультант Плюс». https://clck.ru/36brSB

Судебная практика не отличается единообразием подходов при оценке переписки, не заверенной электронной подписью. Суды, как правило, рассматривают спор, учитывая предшествующую практику сторон, их поведение по исполнению обязательств после переписки, дают оценку с учетом совершения конклюдентных действий, последующего одобрения и т. п.

Участникам гражданского оборота хотелось порекомендовать внимательно относиться к ведению переписки, по наиболее важным контрактам все-таки заключать договоры/соглашения о порядке дистанционного взаимодействия путем электронного документооборота.

Для предсказуемости разрешения судебных споров было бы целесообразным принятие разъяснений на уровне Верховного Суда РФ. Основой таких разъяснений должен быть подход, разграничивающий стадии, на которых велась переписка, и установление разных презумпций доказывания легитимности такой переписки.

Для преддоговорной стадии должны быть более жесткие критерии. Переписка без использования электронной подписи не должна рассматриваться в качестве юридически значимой (оферта, акцепт). Исключением, безусловно, должны быть случаи, когда между сторонами заключено соглашение об электронном документообороте.

Такой подход можно обосновать тем, что отправитель еще не вступил в отношения с контрагентом, не подтверждал свою идентификацию каким-либо адресом электронной почты и не должен нести риски того, что с его почты уйдет какое-либо несанкционированное им сообщение. Если же речь идет о последующих стадиях, то здесь можно было бы ввести презумпцию того, что отправленное с адреса электронной почты, указанного в договоре, сообщение признается выражением воли стороны договора.

Изложенное свидетельствует о необходимости выработки четких ориентиров распределения бремени доказывания при разрешении споров относительно оценки «заключенности» договора в ходе дистанционного взаимодействия посредством электронного документооборота.

3. Отдельные аспекты дистанционных сделок, выходящие за пределы частноправового регулирования

Необходимость выделения дистанционных сделок в отдельную категорию обусловлена, помимо прочего, рядом специфических аспектов, находящихся за пределами гражданско-правового регулирования. Некоторые из этих аспектов будут рассмотрены в настоящем разделе работы, не претендуя на полноту исследования.

3.1. Возложение на частных субъектов (носителей информации по дистанционным сделкам) публичных функций

Процесс цифровизации договорной сферы с неизбежностью ставит перед российским законодателем вопрос о возложении публичных функций на частных субъектов, которые являются носителями или хранителями информации о взаимодействии участников договорных отношений в цифровой среде.

Наделение частных субъектов публичными обязанностями не является новым явлением. В подтверждение можно привести несколько примеров из банковской сферы. Это осуществление банками контрольных функций по противодействию легализации (отмыванию) доходов, полученных преступным путем[12], выполнение функции валютного контроля[13].

Публичные функции являются обременительными для кредитных организаций с экономической точки зрения, поскольку требуют дополнительных затрат, не связанных непосредственно с получением дохода. Это вступает в определенное противоречие с их гражданско-правовым статусом как коммерческих организаций, целью деятельности которых является извлечение прибыли. Между тем законодателем данные функции возложены на кредитные организации, и, очевидно, обязанности по их осуществлению должны рассматриваться в качестве неотъемлемой части их правового статуса.

Видимо, аналогичным образом придется решать вопрос и применительно к частным субъектам – правообладателям и хранителям информации о сделках, совершаемых в информационной среде.

В зарубежной литературе отмечается трансформация задач, стоящих перед интернет-провайдерами. «Частные субъекты не только принимают участие в разработке правил для своего сектора, но и несут ответственность за выявление нарушений. Частные субъекты не просто помогают государственному применению права путем внедрения правил; сегодня частные субъекты активно противодействуют нарушениям и разрабатывают стратегии и инструменты для этого» (Tosza, 2021).

В связи с активным развитием дистанционного совершения сделок на законодательном уровне потребуется решать вопрос о возложении на интернет-провайдеров функций, выходящих за пределы их частного интереса. К числу таких функций следует отнести обязанности по хранению и предоставлению информации о сделках, совершенных в сети Интернет (в случае спора между сторонами), а также функции по контролю ряда сделок или операций в целях обеспечения защиты публичных интересов.

3.2. Особенности доказывания по спорам, возникающим из дистанционных сделок

Дистанционный характер взаимодействия участников сделки с применением цифровых технологий на преддоговорном этапе, на стадиях заключения и исполнения договора порождает вопрос о специфике рассмотрения споров, процесса доказывания по таким спорам. Действующее законодательство не устанавливает каких-либо процессуальных особенностей рассмотрения споров, включая сбор и оценку цифровых доказательств, распределение бремени доказывания.

В зарубежной литературе удалось обнаружить достаточно детальное исследование относительно сбора, хранения, доступа к цифровым доказательствам, относящимся к расследованию дорожно-транспортных происшествий. В работе предпринята попытка комплексного исследования целого блока вопросов, касающихся

[12] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. № 115-ФЗ от 07.08.2001 (с изменениями). СПС «Консультант Плюс». https://clck.ru/36brw7

[13] О валютном регулировании и валютном контроле. № 173-ФЗ (с изменениями) от 10.12.2003. СПС «Консультант Плюс». https://clck.ru/36brwh

процесса доказывания аварий на транспорте, включая методы получения и передачи доказательств в цифровой сфере, доступ к данным, роль и ответственность различных заинтересованных лиц (Philip & Saravanaguru, 2022).

Описанная структура построения расследования несчастных случаев с использованием цифровых доказательств представляет интерес не только для сферы криминалистики.

Применительно к доказательствам и доказыванию по гражданским спорам, вытекающим из дистанционных сделок, отметим, что затронутые в указанной выше работе вопросы проверяемости доказательств и доверия сторон к источникам доказательств имеют первостепенное значение.

Представляется, что процедуры признания тех или иных доказательств допустимыми в рамках споров по дистанционным сделкам должны быть урегулированы на уровне закона. При этом стороны своим соглашением должны иметь возможность договориться о способе подтверждения тех или иных фактов в пределах, установленных законом. Установление законодателем этих пределов должно осуществляться с учетом баланса интересов сторон дистанционной сделки, возможной информационной асимметрии.

Еще один важный аспект рассмотрения споров, возникающих по дистанционным сделкам, касается применения судом того или иного стандарта доказывания, особенностей распределения бремени доказывания.

Действующее процессуальное законодательство не содержит определения стандарта доказывания. В юридической литературе высказываются разные точки зрения относительно целесообразности законодательного закрепления данной правовой конструкции (Токарева, 2023).

Между тем анализ судебной практики свидетельствует о том, что суды при разрешении споров вырабатывают подходы по использованию определенных стандартов доказывания применительно к разным категориям споров («баланс вероятностей», «ясные и убедительные доказательства»)[14].

Представляется, что для споров по дистанционным сделкам в части доказывания фактов, основанных на взаимодействии с использованием цифровых технологий, должен быть выработан специальный стандарт доказывания, основанный на учете правового положения участников сделки.

Данный вопрос требует специального исследования. В рамках постановки проблемы для обсуждения можно предложить, что обязанность по предоставлению цифровых доказательств должна возлагаться на сторону, которая является хранителем информации или наиболее тесным образом с лицом, осуществляющим хранение. На эту же сторону должно возлагаться бремя доказывания неизменности документа в случае, если другая сторона ссылается на его искажение. К стороне, которая является хранителем доказательств в цифровой среде, должен применяться стандарт «ясные и убедительные доказательства» применительно к тем обстоятельствам, на которые ссылается эта сторона. К другой же стороне достаточно применять стандарт «баланс вероятностей».

---

[14] Определение Судебной коллегии по экономическим спорам Верховного Суда РФ № 308-ЭС17-6757(2, 3) от 06.08.2018 по делу № А22-941/2006. СПС «Консультант Плюс». ссылку; Определение Судебной коллегии по экономическим спорам Верховного Суда РФ № 305-ЭС16-18600(5–8) от 30.09.2019 по делу № А40-51687/2012. СПС «Консультант Плюс». https://clck.ru/36brxP

3.3. Использование потенциала искусственного интеллекта, смарт-контрактов при дистанционном взаимодействии участников договорных отношений

Отдельные сферы бизнеса несут в себе риски и неудобства для ключевых участников, которые можно было бы решить в рамках использования тех возможностей, которые заложены в цифровых технологиях, но не в полном объеме используются на практике.

В качестве примера приведем строительство различных объектов, имеющих коммерческую привлекательность (многоквартирных жилых домов, гостиниц, бизнес-центров и т. п.). К ключевым участникам проекта по строительству объекта можно отнести девелопера, застройщика, проектировщика, технического заказчика, генерального подрядчика, инвесторов, страховщиков, кредитную организацию и т. п.

На текущий момент отношения между участниками проекта по строительству объекта строятся в рамках двусторонних договорных обязательств примерно следующим образом:

– девелопер/застройщик – проектировщик;
– застройщик – инвестор/инвесторы;
– застройщик – генеральный подрядчик;
– генеральный подрядчик – подрядчик;
– генеральный подрядчик – поставщик;
– застройщик – технический заказчик;
– застройщик – кредитная организация;
– застройщик – страховая организация.

Для участников проекта важным является получение объективных и проверенных данных:

– на начальном этапе – относительно состояния рынка недвижимости, конъюнктуры спроса и предложения на аналогичные объекты, тенденций на этом рынке, а также относительно стоимости строительства и перспектив ее изменения;

– на последующих этапах – относительно рыночных изменений тех параметров, которые были заложены в бизнес-модель проекта на начальном этапе, а также степени готовности объекта в сопоставлении с установленным графиком.

Существующая практика свидетельствует, что сбор, проверка, анализ информации проводятся разными субъектами, что негативно влияет на инвестиционный климат.

Так, девелопер на самом начальном этапе должен оценить перспективы развития территории, определиться с концепцией будущего объекта строительства, провести экономический анализ, включая прогнозирование доходности инвестиций, подобрать соответствующий земельный участок, обеспечить разработку проектной документации.

На этапе получения банковского финансирования все параметры, заложенные в бизнес-модель проекта, проверяются и оцениваются кредитной организацией, которая прилагает дополнительные усилия для получения объективных данных из независимых источников, использует свои собственные методики для оценки рисков проекта. Инвесторы, принимая решение о вложениях в проект, также заинтересованы в получении объективной информации и правильной оценке потенциала проекта.

В последующем, на этапе строительства, все участники непосредственно заинтересованы в достоверной информации о ходе реализации проекта, влиянии на проект тех изменений, которые затрагивают параметры, заложенные в бизнес-модели проекта.

Занимаясь сбором, анализом сведений, ни один из субъектов не может быть уверен в их объективности, правильности проведенной им оценки и адекватности принимаемого риска. Это создает неуверенность у инвесторов относительно окупаемости проекта, влечет длительность рассмотрения кредитной организацией заявки на получение банковского кредитования и установление условий кредитования, исходя из консервативных подходов, направленных на хеджирование рисков, включая риск недостоверности информации.

Таким образом, указанные обстоятельства приводят в сфере строительства к тому, что предприниматели в конечном итоге отказываются от реализации интересных идей, исходя из сложности доказывания инвесторам и кредитующему банку перспектив окупаемости и получения дохода.

Аналогичная ситуация складывается и в иных сферах, где бизнес-процесс основан на производственной и финансовой интеграции с участием большого числа субъектов. В литературе отмечается, что в последние годы появилось финансирование цепочки поставок – финансовая деятельность, производная от производственной цепочки реального сектора экономики. Предлагается применение смарт-контрактов в цепочке поставок. Это позволит решить проблему доступа к кредитным ресурсам малым и средним предприятиям (Zhang et al., 2021). Цепочка поставок и все ее логические взаимосвязи должны быть полностью отображены в блокчейн-сети, чтобы обеспечить прозрачность, подлинность и проверяемость каждой из них (Dietrich et al., 2020).

Представляет интерес исследование, проведенное Will Serrano, которым представлены модель валидации и верификации (V & V), рынок данных на основе искусственного интеллекта (AI), который состоит из трех уровней верификации, каждая из которых имеет ценность для определенных участников проекта. Так, серебряная проверка имеет значение, в частности, для страховщиков. Она включает анализ данных в целях выявления отклонений от диапазона или правила добавленной стоимости. Третий уровень – «Gold verification: прогнозирование данных на основе нескольких алгоритмов искусственного интеллекта и Модели машинного обучения (ML)» – имеет значение для города или управляющих активами и городских застройщиков (Serrano, 2022).

Изложенное позволяет сделать вывод, что внедрение информационной интерактивной модели с проверкой данных через блокчейн и смарт-контракт позволит решить вопросы доверия между участниками бизнес-процессов с высокой степенью производственной интеграции, обеспечит возможность эффективного управления и коммерциализации проекта или инвестиций.

Правовой механизм внедрения подобной информационно-экономической модели проекта или цепочек поставок должен включать, на наш взгляд, в качестве начального этапа закрепление в актах публичного права правил, предусматривающих:

– разработку требований к искусственному интеллекту для решения указанных выше задач;

– проведение экспертизы на предмет корректности задач перед искусственным интеллектом и признания результатов их решения. Экспертиза должна быть проведена с участием профильных государственных органов (в сфере строительства и органов надзора в сфере банковской деятельности и т. п.).

Отношения между субъектами частного права могут строиться с использованием модели дистанционных сделок, предметом которых будет являться использование данных, содержащихся в информационной модели проекта без права внесения туда корректировок, удаления данных и т. п.

Более детальный анализ предлагаемого варианта использования дистанционных сделок на текущий момент сделать не представляется возможным в силу отсутствия разработки базовых подходов даже на уровне проектов нормативных актов либо разработок доктрины в данной области публичного права.

Выводы

1. Развитие цифровых технологий порождает новые дистанционные способы совершения сделок, а также наполняет новым содержанием традиционные для гражданского права процедуры заключения договора путем обмена сообщениями.

2. Действующее законодательство не выделяет «дистанционный договор» в качестве правовой конструкции (модели) гражданско-правового договора.

Между тем применение цифровых технологий при дистанционном способе взаимодействия участников договорных отношений порождает значительное число проблем, которые могли бы быть решены в рамках специальной договорной конструкции «дистанционного договора» с установлением специального правового режима.

3. Автором выделяются следующие признаки «дистанционного договора»:

– заключение договора без личного присутствия сторон в момент выражения воли в месте заключения договора;

– использование цифровых технологий при дистанционном характере взаимодействия.

В рамках специального правового режима «дистанционного договора» должны быть решены как минимум следующие вопросы:

– о критериях установления статуса сторон договора, признания одной из них слабой стороной;

– об условиях ответственности сторон, в том числе о применении принципа «строгой» ответственности (независимо от наличия вины), о пределах его применения;

– о том, кто несет риски технологических сбоев, хакерских атак;

– о распределении бремени доказывания между сторонами.

4. В качестве правовой категории наряду с «дистанционным договором» следует выделить и «дистанционные сделки».

При этом базовым понятием должно являться понятие «дистанционного договора», правила о котором могут быть распространены на односторонние дистанционные сделки.

5. Односторонняя сделка может быть квалифицирована в качестве дистанционной сделки при наличии следующих признаков:

– односторонняя сделка является сделкой, требующей восприятия;

– доведение волеизъявления до контрагента осуществляется с использованием цифровых технологий.

6. Необходимость выделения дистанционных сделок в отдельную категорию обусловлена, помимо прочего, рядом специфических аспектов, находящихся за пределами гражданско-правового регулирования. К их числу можно отнести:

– возложение на частных субъектов (носителей информации по дистанционным сделкам) публичных функций;

– особенности доказывания по спорам, возникающим из дистанционных сделок;

– использование потенциала ИИ, смарт-контрактов при дистанционном взаимодействии участников договорных отношений.

Список литературы

Акужинов, А. (2020). Сделки, требующие и не требующие восприятия: теоретическое и практическое основание квалификации. *Цивилистика*, *6*, 124–152. https://www.elibrary.ru/hhnnis

Белов, В. А. (2021). Смарт-контракт: понятие, правовое регулирование, правоприменительная практика, потребительские отношения. *Право и экономика*, *9*, 35–41. https://www.elibrary.ru/zcbdhr

Гринь, О. С. (2019). Трансформации требований к форме договоров с учетом развития цифровых технологий. *Актуальные проблемы российского права*, *6*, 49–57. EDN: https://www.elibrary.ru/whwjyc. DOI: https://doi.org/10.17803/1994-1471.2019.103.6.049-057

Егоров, А. В. (2015). Верховный суд разъяснил понятие сделки. Наступила ли ясность? *Арбитражная практика*, *12*, 29. https://www.elibrary.ru/wmlhlv

Ефимова, Л. Г. (2019). Еще раз о понятии и правовой природе электронной формы сделки. *Lex russica*, *8*, 129–137. EDN: https://www.elibrary.ru/evaoxo. DOI: https://doi.org/10.17803/1729-5920.2019.153.8.129-137

Ефимова, Л. Г., Сиземова, О. Б. (2019). Правовая природа смарт-контракта. *Банковское право*, *1*. EDN: https://www.elibrary.ru/yvaxlv. DOI: https://doi.org/10.18572/1812-3945-2019-1-21-28

Кириллова, Е. А. (2021). Нотариальные сделки в электронной форме: некоторые проблемы практики. *Нотариус*, *5*, 41–43. EDN: https://www.elibrary.ru/uvzbuj. DOI: https://doi.org/10.18572/1813-1204-2021-5-41-43

Козлова, М. Ю., Сергачева, О. А. (2022). Влияние цифровизации на форму договора. *Цивилист*, *1*. https://www.elibrary.ru/edwlwo

Костикова, Г. В. (2022). Электронные сделки: новеллы законодательства. *Хозяйство и право*, *2*, 49–59. EDN: https://elibrary.ru/azafwm. DOI: https://doi.org/10.18572/0134-2398-2022-2-49-59

Кузьмина, А. В., Ломакина, Е. А. (2022). Защита слабой стороны от навязывания несправедливых условий договора, заключаемого в сети Интернет. *Российский юридический журнал*, *4*. EDN: https://elibrary.ru/zcrhpw. DOI: https://doi.org/10.34076/20713797_2022_4_121

Лаптев, В. А., Соловяненко, Н. И. (2022). Дистанционная сделка и электронная подпись: правовая конструкция и форма заключения. *Юрист*, *12*, 16–22. EDN: https://elibrary.ru/qpaihf. DOI: https://doi.org/10.18572/1812-3929-2022-12-16-22

Михайлова, А. С. (2020). К вопросу об отдельных аспектах применения электронных технологий в процессе удостоверения завещаний. *Нотариус*, *7*, 28–31. EDN: https://elibrary.ru/onmssw. DOI: https://doi.org/10.18572/1813-1204-2020-7-28-31

Овчинникова, Ю. С. (2022). Цифровизация страховых услуг: защита слабой стороны договора и частной жизни. *Имущественные отношения в Российской Федерации*, *3*, 73–81. EDN: https://elibrary.ru/sywrgk. DOI: http://dx.doi.org/10.24412/2072-4098-2022-3246-73-81

Савельев, А. И. (2016). Договорное право 2.0: «умные» контракты как начало конца классического договорного права. *Вестник гражданского права*, *3*, 32–60. https://elibrary.ru/whffcx

Савельева, Т. А. (2022). Цифровизация: защита слабой стороны договора. В сб. И. Р. Бегишев, Е. А. Громова, М. В. Залоило, И. А. Филипова, А. А. Шутова, *Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции* (г. Казань, 23 сентября 2022 г.) (в 6 т. Т. 2, с. 478–490). Казань: Изд-во «Познание» Казанского инновационного университета. EDN: https://elibrary.ru/jsixfm. DOI: http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

Токарева, Е. В. (2023). О месте «стандарта доказывания» в цивилистическом процессе. *Вестник арбитражной практики*, *2*, 35–40. https://clck.ru/36m8nU

Уткин, В. В. (2022). К вопросу о правовом регулировании смарт-контрактов. *Хозяйство и право*, *11*, 92–98. http://dx.doi.org/10.18572/0134-2398-2022-11-92-98

Филипова, И. А. (2023). Искусственный интеллект: горизонт влияния на трудовые правоотношения. *Юрист*, *3*, 23–28. http://dx.doi.org/10.18572/1812-3929-2023-3-23-28

Цепов, Г. В., Иванов, Н. В. (2022). К цивилистической теории смарт-контрактов. *Закон*, *3*, 149–172. http://dx.doi.org/10.37239/0869-4400-2022-18-3-149-172

Челышева, Н. Ю. (2022). Концепция правового регулирования смарт-контракта в гражданском праве. *Право и экономика*, *7*, 32–36. https://elibrary.ru/mjmzfn

Чурилов, А. Ю. (2020). К проблеме понятия и правовой природы смарт-контракта. *Юрист*, *7*, 25–30. EDN: https://elibrary.ru/bouxik. https://doi.org/10.18572/1812-3929-2020-7-25-30

Шелепина, Е. А. (2021). Тенденции правового регулирования электронного документооборота в национальном гражданском праве. *Право и цифровая экономика*, *1*, 26–35. EDN: https://elibrary.ru/qhhhgi. DOI: http://dx.doi.org/10.17803/2618-8198.2021.11.1.026-035

Яценко, Т. С. (2019). Проблемы правового регулирования электронных завещаний в зарубежных странах. *Нотариус*, *7*, 42–44. https://elibrary.ru/idsjmj

Aquilina, S. J., Casino, F., Vella, M., Ellul, J., & Patsakis, C. (2021). EtherClue: Digital investigation of attacks on Ethereum smart contracts. *Blockchain: Research and Applications*, *2*(4), 100028. https://doi.org/10.1016/j.bcra.2021.100028

Dietrich, F., Palm, D., & Louw, L. (2020). Smart contract based framework to increase transparency of manufacturing networks. *Procedia CIRP*, *91*, 278–283. https://doi.org/10.1016/j.procir.2020.02.177

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142, https://doi.org/10.1016/j.bcra.2023.100142

Hsain, Ya. Ait, Laaz, N., & Mbarki, S. (2021). Ethereum's Smart Contracts Construction and Development using Model Driven Engineering Technologies: a Review. *Procedia Computer Science*, *184*, 785–790, https://doi.org/10.1016/j.procs.2021.03.097

Kennedy, G. (2023). The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law. *Computer Law & Security Review*, *49*, 105832. https://doi.org/10.1016/j.clsr.2023.105832

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *15*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Lim, A., & Pan, E. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Philip, A. O., & Saravanaguru, R. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Serrano, W. (2022). Verification and Validation for data marketplaces via a blockchain and smart contracts. *Blockchain: Research and Applications*, *3*(4), 100100. https://doi.org/10.1016/j.bcra.2022.100100

Tărchilă, P., & Nagy, M. (2015). Comparative Approach of the Electronic Contract and Classical Contract, in Teaching The Content of the New Civil Code in Romania. *Procedia – Social and Behavioral Sciences*, *191*, 464–468. https://doi.org/10.1016/j.sbspro.2015.04.588

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*, *43*, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Van Rompaey, L., Jønsson, R., & Jørgensen, K. E. (2022). Designing lawful machine behaviour: Roboticists' legal concerns. *Computer Law & Security Review*, *47*, 105711. https://doi.org/10.1016/j.clsr.2022.105711

Zhang, TianLin, Li, JinJiang, & Jiang, Xinbo. (2021). Supply chain finance based on smart contract. *Procedia Computer Science*, *187*, 12–17. https://doi.org/10.1016/j.procs.2021.04.027

Сведения об авторе

Савельева Татьяна Александровна – кандидат юридических наук, доцент кафедры гражданского права, Новосибирский юридический институт (филиал) Томского государственного университета
Адрес: 630007, Российская Федерация, г. Новосибирск, ул. Советская, 7
E-mail: sta.sd@bk.ru
ORCID ID: https://orcid.org/0009-0000-9831-665X
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1195986

Конфликт интересов

Автор сообщает 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: 10.27.41 / Сделки
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 31 июля 2023 г.
Дата одобрения после рецензирования – 21 августа 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.46

Remote Methods of Conducting Transactions Using Digital Technologies

Tatyana A. Savelyeva

Novosibirsk Law Institute (branch) of Tomsk State University
Novosibirsk, Russia

Keywords

artificial intelligence,
balance of interests,
blockchain,
digital technologies,
distant contract,
distant transaction,
electronic document,
information technologies,
law,
smart contract

Abstract

Objective: to substantiate the need to identify new contractual constructs (models) taking into account the specific relations associated with the use of remote method of contract conclusion through digital technologies and to study the possible risks for their participants.

Methods: along with special legal methods, the method of critical analysis was fundamental for the research process, which allowed us to evaluate and interpret the main sources and norms of civil law in relation to distant transactions. It also allowed assessing the current state of legislation in this area in the context of developing processes of digitalization and technologization of civil-law relations.

Results: a critical analysis of the current state of legal regulation of remote ways of concluding contracts is presented, their classification is given. It is concluded that the digital technologies development gives rise to new remote ways of transactions, as well as fills with new content the procedures of contract conclusion, traditional for civil law. The expediency of singling out the concept of a "distant transaction" as a legal category in order to create a special civil-law regime is substantiated, and the basic concept being that of a "distant contract". Certain types of distant contracts are analyzed to substantiate the need for special legal regimes in cases when the distant method of contract conclusion is combined with the use of digital technologies. It poses such problems as the distribution of risks of technological failures, hacker attacks, compliance with the balance of interests of the parties taking into account information asymmetry, and the need to protect the weaker party.

Scientific novelty: an attempt is made to define such concepts as a "distant contract" and a "distant transaction" and to identify their features. The expediency is substantiated of considering a distant contract as a separate legal construction (model) of the contract. Within this framework, a special legal regime should be developed and fixed, which can be extended to unilateral distant transactions. The problems of legal regulation caused by the use of information technologies are formulated, and legal constructions for their solution are proposed.

Practical significance: the final conclusions and proposals can be used both in contractual practice by the participants of civil turnover and for the normative consolidation of the concept and features of "distant contract", "distant transaction". A special legal regime can be created, taking into account the specificity generated by the use of digital technologies.

For citation

Savelyeva, T. A. (2023). Remote Methods of Conducting Transactions Using Digital Technologies. *Journal of Digital Technologies and Law, 1*(4), 1058–1086. https://doi.org/10.21202/jdtl.2023.46

References

Akuzhinov, A. (2020). Transactions requiring and not requiring discernment: theoretical and practical basis for qualification. *Tsivilistika*, *6*, 124–152. (In Russ.).

Aquilina, S. J., Casino, F., Vella, M., Ellul, J., & Patsakis, C. (2021). EtherClue: Digital investigation of attacks on Ethereum smart contracts. *Blockchain: Research and Applications*, *2*(4), 100028. https://doi.org/10.1016/j.bcra.2021.100028

Belov, V. A. (2021). Smart contract: concept, legal regulation, law enforcement practice, consumer relations. *Pravo i ehkonomika*, *9*, 35–41. (In Russ.).

Chelysheva, N. Yu. (2022). Concept of legal regulation of smart contract in civil law. *Pravo i ehkonomika*, *7*, 32–36. (In Russ.).

Churilov, A. Yu. (2020). On the concept and legal nature of a smart contract. *Yurist*, *7*, 25–30. https://doi.org/10.18572/1812-3929-2020-7-25-30

Dietrich, F., Palm, D., & Louw, L. (2020). Smart contract based framework to increase transparency of manufacturing networks. *Procedia CIRP*, *91*, 278–283. https://doi.org/10.1016/j.procir.2020.02.177

Efimova, L. G. (2019). On the Concept and Legal Nature of the Electronic Form of the Transaction. *Lex Russica*, *8*, 129–137. (In Russ.) https://doi.org/10.17803/1729-5920.2019.153.8.129-137

Efimova, L. G., & Sizemova, O. B. (2019). Legal nature of a smart contract. *Banking Law*, *1*. (In Russ.). https://doi.org/10.18572/1812-3945-2019-1-21-28

Egorov, A. V. (2015). The Supreme Court has clarified the concept of a transaction. Has it become clearer? *Arbitrazhnaya praktika*, *12*, 29. (In Russ.).

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3), 100142. https://doi.org/10.1016/j.bcra.2023.100142

Filipova, I. A. (2023). Artificial Intelligence: The Degree of Influence on Labor Relations. *Yurist*, *3*, 23–28. (In Russ.). http://dx.doi.org/10.18572/1812-3929-2023-3-23-28

Grin, O. S. (2019). Transformation of contract form requirements based on the development of digital technologies. *Actual Problems of Russian Law*, *6*, 49–57. (In Russ.). https://doi.org/10.17803/1994-1471.2019.103.6.049-057

Hsain, Ya. Ait, Laaz, N., & Mbarki, S. (2021). Ethereum's Smart Contracts Construction and Development using Model Driven Engineering Technologies: a Review. *Procedia Computer Science*, *184*, 785–790. https://doi.org/10.1016/j.procs.2021.03.097

Kennedy, G. (2023). The "Gold" Standard – China finalises the long-anticipated Standard Contract under the Personal Information Protection Law. *Computer Law & Security Review*, *49*, 105832. https://doi.org/10.1016/j.clsr.2023.105832

Kirillova, E. A. (2021). Notary transactions in electronic form: some problems of practice. *Notary*, *5*, 41–43. (In Russ.). https://doi.org/10.18572/1813-1204-2021-5-41-43

Kirli, D., Couraud, B., Robu, V., Salgado-Bravo, M., Norbu, S., Andoni, M., Antonopoulos, I., Negrete-Pincetic, M., Flynn, D., & Kiprakis, A. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. *Renewable and Sustainable Energy Reviews*, *15*, 112013. https://doi.org/10.1016/j.rser.2021.112013

Kostikova, G. V. (2022). Electronic transactions: legislative novelties. *Khozyaistvo i pravo*, *2*. (In Russ.). https://doi.org/10.18572/0134-2398-2022-2-49-59

Kozlova, M. Yu., & Sergacheva, O. A. (2022). The impact of digitalization on the form of a contract. *Tsivilist*, *1*. (In Russ.).

Kuzmina, A. V., & Lomakina, E. A. (2022). Protection of the weak party from the imposition of unfair terms of the contract concluded on the Internet. *Russian Juridical Journal*, *4*. (In Russ.). https://doi.org/10.34076/20713797_2022_4_121

Laptev, V. A., & Solovyanenko, N. I. (2022). A Distance Transaction and an Electronic Signature: The Legal Structure and the Form of Conclusion. https://doi.org/10.18572/1812-3929-2022-12-16-22

Lim, A., & Pan, E. (2021). 'Toward a Global Social Contract for Trade' – a Rawlsian approach to Blockchain Systems Design and Responsible Trade Facilitation in the New Bretton Woods era. *Journal of Responsible Technology*, *6*, 100011. https://doi.org/10.1016/j.jrt.2021.100011

Mikhaylova, A. S. (2020). On some aspects of electronic technology application in will attestation. *Notary*, *7*, 28–31. (In Russ.). https://doi.org/10.18572/1813-1204-2020-7-28-31

Ovchinnikova, Yu. S. (2022). Digitalization of insurance services: protection of the weak side of the contract and private life. *Property Relations in the Russian Federation*, *3*, 73–81. (In Russ.). http://dx.doi.org/10.24412/2072-4098-2022-3246-73-81

Philip, A. O., & Saravanaguru, R. K. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. *Journal of King Saud University – Computer and Information Sciences*, *34*(7), 4031–4046. https://doi.org/10.1016/j.jksuci.2022.06.001

Savelyev, A. I. (2016). Contract law 2.0: "smart contracts" and the beginning of the end of the classic contract law. *Civil Law Review*, *3*, 32–60. (In Russ.).

Savelyeva, T. A. (2022). Digitalization: protection of the weak side of the contract. In I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, & A. A. Shutova, *Digital Technologies and Law: collection of works of the I International Scientific and Practical Conference* (Kazan, September 23, 2022). (In 6 vol. Vol. 2, pp. 478–490). Kazan: Poznaniye Publishers of Kazan Innovative University. http://dx.doi.org/10.21202/978-5-8399-0769-0_2022_2_556

Serrano, W. (2022). Verification and Validation for data marketplaces via a blockchain and smart contracts. *Blockchain: Research and Applications*, *3*(4), 100100. https://doi.org/10.1016/j.bcra.2022.100100

Shelepina, E. A. (2021). Trends of legal regulation of electronic document flow in national civil law. *Law and Digital Economy*, *1*, 26–35 (In Russ.). http://dx.doi.org/10.17803/2618-8198.2021.11.1.026-035

Tărchilă, P., & Nagy, M. (2015). Comparative Approach of the Electronic Contract and Classical Contract, in Teaching The Content of the New Civil Code in Romania. *Procedia – Social and Behavioral Sciences*, *191*, 464–468. https://doi.org/10.1016/j.sbspro.2015.04.588

Tokareva, E. V. (2023). On the place of the "standard of proof" in the civilistic procedure. *Vestnik arbitrazhnoi praktiki*, *2*, 35–40. (In Russ.). https://clck.ru/36m8nU

Tosza, S. (2021). Internet service providers as law enforcers and adjudicators. A public role of private actors. *Computer Law & Security Review*, *43*, 105614. https://doi.org/10.1016/j.clsr.2021.105614

Tsepov, G. V., Ivanov, N. V. (2022). Towards a Civil-Law Theory of Smart Contracts. *Zakon*, *3*, 149–172. (In Russ.). https://doi.org/10.37239/0869-4400-2022-18-3-149-172

Utkin, V. V. (2022). On the legal regulation of smart contracts. *Economy and Law*, *11*, 92–98. http://dx.doi.org/10.18572/0134-2398-2022-11-92-98

Van Rompaey, L., Jønsson, R., & Jørgensen, K. E. (2022). Designing lawful machine behaviour: Roboticists' legal concerns. *Computer Law & Security Review*, *47*, 105711. https://doi.org/10.1016/j.clsr.2022.105711

Yatsenko, T. S. (2019). Problems of legal regulation of electronic wills in foreign countries. *Notary*, 7, 42–44. (In Russ.).

Zhang, TianLin, Li, JinJiang, & Jiang, Xinbo. (2021). Supply chain finance based on smart contract. *Procedia Computer Science*, *187*, 12–17. https://doi.org/10.1016/j.procs.2021.04.027

Author information

Tatyana A. Savelyeva – Cand. Sci. (Law), Associate Professor of Department of Civil Law, Novosibirsk Law Institute (branch) of Tomsk State University
Address: 7 Sovetskaya Str., 630007 Novosibirsk, Russian Federation
E-mail: sta.sd@bk.ru
ORCID ID: https://orcid.org/0009-0000-9831-665X
РИНЦ Author ID: https://elibrary.ru/author_items.asp?authorid=1195986

Conflicts of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – July 31, 2023
Date of approval – August 21, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:341.492:343.11
EDN: https://elibrary.ru/dtiann
DOI: https://doi.org/10.21202/jdtl.2023.47

Цифровые преобразования южноафриканского правового ландшафта

Уильям Манга Мокофе

Верховный Суд Южно-Африканской Республики
г. Ист-Лондон, Южно-Африканская Республика

Ключевые слова

законодательство,
защита персональных данных,
искусственный интеллект,
киберпреступность,
онлайн-разрешение споров,
право интеллектуальной собственности,
право,
судебная практика,
цифровые технологии,
Южная Африка

Аннотация

Цель: Южная Африка является страной с большим потенциалом интенсивного развития благодаря стремительному росту и внедрению цифровых технологий. Активно формирующаяся цифровая среда трансформирует законодательную базу, которая в свою очередь оказывает влияние на цифровую среду. Это преобразующее взаимоотношение обусловило направленность исследования на выявление адаптивности правовой системы перед лицом динамичных изменений и путей эволюции правового ландшафта в условиях цифровизации и технологического прогресса.

Методы: изучение изменяющегося правового ландшафта требует междисциплинарного подхода, сочетающего юридический анализ с идеями из областей социологии, экономики и др. При этом с помощью формально-юридического метода исследуются ключевые правовые акты, формирующие цифровую среду Южной Африки и определяющие возможности и проблемы взаимодействия цифровых технологий и южноафриканского права.

Результаты: в работе дается представление о том, как правовая система Южной Африки решает цифровые проблемы; оценивается интеграция цифровых новаций в правовую систему; подчеркивается преобразующее влияние цифровых технологий на традиционные юридические процессы, охватывающие сбор доказательств, разрешение споров и доступ к правосудию; оценивается роль цифровых технологий в повышении эффективности юридических процессов.

Научная новизна: исследование вносит вклад в продолжающуюся дискуссию о сложной взаимосвязи между цифровыми технологиями и законодательством Южной Африки; показано, как южноафриканское

право справляется с цифровыми сложностями; обосновываются новые идеи о трансформации традиционной правовой парадигмы в результате цифровизации, ее последствий для судопроизводства и доступа к правосудию. При углублении в адаптацию, проблемы и инновации, возникающие на пересечении права, технологий и цифровизации, происходит понимание того, как южноафриканское право ориентируется в динамичной цифровой среде.

Практическая значимость: адаптация правового ландшафта к цифровизации и технологическим достижениям имеет решающее значение для обеспечения быстрого технологического прогресса и требует сотрудничества между государственными органами, гражданским обществом, экспертами в области права и технологий. Исследование содержит ценные рекомендации и предложения для политиков, юристов-практиков и заинтересованных сторон, формирующих правовую экосистему Южно-Африканской Республики, решающих проблемы обеспечения конфиденциальности персональных данных, повышения эффективности электронных взаимодействий и противодействия киберпреступности. Подчеркивается важность внедрения технологического прогресса при одновременном соблюдении надежных правовых гарантий.

Для цитирования

Мокофе, У. М. (2023). Цифровые преобразования южноафриканского правового ландшафта. *Journal of Digital Technologies and Law*, *1*(4), 1087–1104. https://doi.org/10.21202/jdtl.2023.47

Содержание

Введение

В современном мире сложное взаимодействие цифровых технологий и нормативно-правовой базы породило новые вызовы и возможности, которые нигде не проявляются так ярко, как в условиях Южной Африки. Стремительное развитие цифровых технологий привело к перестройке общества, экономики и структур управления,

коренным образом изменив способы общения, совершения сделок и взаимодействия людей (Mokofe & van Eck, 2021). Эти преобразования вызывают настоятельную необходимость тщательного изучения адаптивности правовых систем к этим динамичным изменениям.

Основная цель данного исследования – изучить реакции и адаптации южноафриканского права к стремительному развитию цифровых технологий, а также оценить широкие последствия этой адаптации. Взаимосвязь этих сфер не случайна; она отражает симбиотические отношения, в которых правовая система стремится регулировать и использовать потенциал цифровых технологий, а цифровые технологии, в свою очередь, бросают вызов традиционно сложившимся правовым нормам (Adams & Adeleke, 2020).

Цифровой ландшафт включает в себя широкий спектр технологий, начиная от вездесущих смартфонов и Интернета и заканчивая более специализированными областями, такими как блокчейн, искусственный интеллект (далее – ИИ) и интернет вещей (IoT). Каждая из этих технологий несет в себе свой набор возможностей и сложностей, переплетаясь с различными аспектами права, от защиты данных и конфиденциальности до интеллектуальной собственности и киберпреступности (Mokofe & van Eck, 2022; Swales, 2021). Следовательно, изучение этого ландшафта требует междисциплинарного подхода, сочетающего юридический анализ с изучением технологий, социологии, экономики и других аспектов.

Данное исследование сосредоточивается в первую очередь на правовых актах, регулирующих цифровую сферу в Южно-Африканской Республике (далее – ЮАР). Принятие таких законов, как Закон о защите персональной информации (Protection of Personal Information Act, POPIA)[1] и Закон об электронных коммуникациях и сделках (Electronic Communications and Transactions Act, ECTA)[2], является примером активных усилий государства по созданию правовых ориентиров для цифровой эпохи. Эти законы направлены на то, чтобы распространение цифровых технологий не сопровождалось нарушением прав личности, конфиденциальности данных и безопасности.

Кроме того, цифровой ландшафт не знает географических границ, что создает уникальные юрисдикционные проблемы. Киберпреступность, часто организуемая из удаленных друг от друга мест, заставляет правовые системы решать сложные задачи транснационального правоприменения и сотрудничества (Mtuze, 2022; Swales, 2022). Такая глобальная взаимосвязь приводит к необходимости международного сотрудничества, а также разработки правовых инструментов, способных эффективно решать проблемы, порождаемые новыми технологиями.

Помимо нормативно-правовых аспектов, цифровая трансформация изменяет традиционные правовые процедуры. Внедрение цифровых доказательств, использование искусственного интеллекта, появление онлайн-платформ для разрешения споров – все это меняет саму структуру судебного процесса (De Sousa et al., 2021). Эти изменения не только повышают эффективность в юридической сфере, но и требуют критической оценки их влияния на традиционные концепции правосудия и надлежащих правовых процедур.

---

1 Copyright Amendment Act, No. 9 of 2019.

2 Electronic Communications and Transactions Act, No. 25 of 2002.

Интеграция цифровых технологий в правовую систему Южно-Африканской Республики представляет собой многогранный дискурс, объединяющий технологии, право и общество (Botha et al., 2017). Цель данного исследования – изучить этот динамический ландшафт и пролить свет на сложную взаимосвязь между правовыми нормами и технологическими достижениями. Рассматривая адаптации, проблемы и инновации, возникающие в этой связи, данное исследование призвано внести вклад в комплексное понимание того, как право Южно-Африканской Республики ориентируется в динамичном ландшафте цифровой эпохи.

1. Адаптация законодательства Южно-Африканской Республики к быстрому развитию цифровых технологий

Развитие цифровых технологий и правового ландшафта в Южно-Африканской Республике привело к возникновению сложных динамических отношений, требующих оперативного реагирования и адаптации правовой базы. Поскольку цифровые технологии продолжают влиять на традиционные нормы и способы функционирования, право Южно-Африканской Республики претерпело ряд значительных изменений. Все они направлены на решение многогранных проблем и использование возможностей, возникающих в результате смены парадигмы (Naude & Papadopoulos, 2016). Рассмотрим эти динамичные изменения ниже.

2. Защита данных и неприкосновенность частной жизни

Одна из наиболее заметных адаптаций произошла в сфере защиты данных и конфиденциальности. Принятие Закона о защите персональной информации (POPIA)[3] стало важнейшим ответом на растущую оцифровку персональных данных. Закон устанавливает всеобъемлющую правовую базу для сбора, обработки и хранения персональных данных, призванную обеспечить соблюдение прав человека в цифровую эпоху. Налагая строгие обязательства на операторов контроля и обработки данных, законодатель постарался найти баланс между технологическими инновациями и защитой частной жизни.

Стремительная интеграция цифровых технологий в повседневную жизнь существенно повлияла на проблемы защиты данных и неприкосновенности частной жизни. Среди законодательных мер, принятых в Южной Африке в ответ на эти вызовы, Закон о защите персональной информации занимает первое место. В условиях растущей оцифровки персональной информации и распространения онлайн обмена данными он играет важнейшую роль, направленную на гармонизацию прав личности и технологических достижений в цифровую эпоху.

Принятие этого закона явилось результатом комплексных усилий по созданию правовой базы, способной регулировать сбор, обработку и хранение персональных данных, сохраняя при этом неприкосновенность частной жизни (Adams & Adeleke, 2020; Bronstein, 2022). По сути, это свидетельствует о признании данных как ценности, защита которой требует надежных правовых механизмов. Закон содержит целый ряд положений, определяющих права субъектов данных и обязанности операторов по контролю и обработке данных (Naude & Papadopoulos, 2016).

[3] Protection of Personal Information Act, No. 4 of 2013.

Налагая жесткие обязательства на организации, работающие с персональными данными, закон стремится установить хрупкое равновесие между развитием инноваций и защитой частной жизни (Malgieri & Comandé, 2017). Его положения направлены на обеспечение прозрачности и подотчетности, обязывая операторов данных получать явно выраженное согласие субъектов на обработку их данных, раскрывать информацию об использовании данных и применять адекватные меры безопасности для предотвращения нарушений.

Принятие этого закона стало также ответом на глобальную тенденцию регулирования защиты данных, что подчеркивает стремление ЮАР привести свой правовой ландшафт в соответствие с международными стандартами (Adams & Adeleke, 2020). Введение закона имеет далеко идущие последствия для компаний, работающих в цифровой сфере, требуя от них пересмотра практики управления данными и создания механизмов ее соблюдения.

Кроме того, принятие Закона о защите персональной информации представляет собой важнейшее изменение южноафриканского законодательства на фоне растущих проблем, связанных с защитой данных и неприкосновенности частной жизни в условиях все большей цифровизации. Обеспечивая надежную правовую базу, задающую тон ответственному управлению данными и сохранению конфиденциальности, законодательство стремится гармонизировать технологические инновации с основными положениями в области прав человека.

3. Законодательство в области киберпреступности

В связи с ростом киберпреступности южноафриканское законодательство было реформировано таким образом, чтобы охватить целый ряд правонарушений и наказаний, связанных с цифровыми преступлениями. Закон о киберпреступлениях (Cybercrimes Act)[4] играет важную роль, криминализируя широкий спектр деяний, включая хакерство, кражу личных данных и кибербуллинг. Этот закон свидетельствует о признании особого рода проблем, связанных с преступлениями в сфере цифровых технологий, и необходимости создания правовой базы, позволяющей эффективно бороться с такими преступлениями, защищая при этом права граждан в сфере цифровых технологий.

Резкое увеличение числа киберугроз подтолкнуло к существенному пересмотру законодательства страны. По мере развития цифровых технологий южноафриканские законодатели осознали острую необходимость адаптации правовой базы для эффективного противодействия киберпреступности. В связи с развитием ситуации был принят Закон о киберпреступлениях, ставший важнейшим шагом на пути укрепления потенциала страны в борьбе со всем спектром цифровых преступлений.

Закон о киберпреступности, являясь важным законодательным актом, представляет собой инструментальный ответ на многогранную природу киберпреступности. Благодаря комплексному подходу к решению этой проблемы закон отходит от традиционных правовых парадигм, предусматривая уголовную ответственность за широкий спектр киберпреступлений. Под действие закона подпадают различные виды деятельности – от хакерства и кражи личных данных до кибербуллинга, что подчеркивает решимость правовой системы Южно-Африканской Республики адаптироваться к современным условиям (Roos, 2020).

[4] Cybercrimes Act, No. 19 of 2020.

Охватывая разнообразные составы киберпреступлений, закон отражает тонкое понимание меняющегося ландшафта цифровых угроз и необходимость многостороннего правового реагирования (Malgieri & Comandé, 2017). В законе признается, что киберпреступность выходит за рамки финансового мошенничества и охватывает действия, ставящие под угрозу частную жизнь, безопасность и благополучие людей в цифровой сфере. Таким образом, закон соответствует международным тенденциям в области законодательства о киберпреступности и демонстрирует стремление ЮАР к укреплению кибербезопасности (de Bruyn, 2014).

Принятие Закона о киберпреступлениях свидетельствует о стратегическом сдвиге в правовом регулировании, признающем особые проблемы и сложности, связанные с цифровыми преступлениями. Этот закон не только направлен на наказание преступников, но и подчеркивает необходимость обеспечения цифровых прав граждан (Van Niekerk, 2018). Устанавливая наказания, соразмерные тяжести преступлений, закон направлен на сдерживание потенциальных правонарушителей и одновременно создает прочную основу для эффективной борьбы правоохранительных органов с киберпреступностью.

Кроме того, принятие Закона о киберпреступлениях свидетельствует об активном подходе ЮАР к формированию правовой базы для противодействия растущей угрозе цифровых преступлений. Благодаря своей всеобъемлющей сфере действия закон подчеркивает динамичный характер киберугроз и необходимость принятия надежных законодательных мер. По мере развития цифрового ландшафта данный закон закладывает основу для защиты цифровых данных физических лиц и способствует созданию безопасной цифровой среды (Van Niekerk, 2017).

4. Электронные транзакции

Закон об электронных сделках (Electronic Communications and Transactions Act, далее – ECTA) является ответом Южно-Африканской Республики на цифровую трансформацию коммерческой деятельности. Обеспечивая юридическое признание электронных подписей, договоров и актов коммуникации, ECTA способствует росту электронной коммерции и электронных сделок, гарантируя их действительность и возможность принудительного исполнения. Эта инновация отвечает растущей распространенности цифровых взаимодействий и направлена на обеспечение правовой определенности в условиях постоянно меняющегося цифрового ландшафта.

В связи с цифровой революцией, изменившей коммерческие взаимодействия и сделки, южноафриканское законодательство заняло активную позицию, приняв ECTA. Этот закон представляет собой комплексный ответ на вызовы и возможности, возникающие в связи с цифровой трансформацией коммерции, и свидетельствует о стремлении страны создать юридически обоснованную среду для электронного взаимодействия.

Принятие ECTA подчеркивает осознание того, что традиционные способы торговли эволюционируют по мере интеграции цифровых технологий. Учитывая стремительный рост электронной коммерции, данный закон устанавливает юридическую силу электронных подписей, договоров и актов коммуникации, а также гарантирует, что электронные сделки являются действительными, подлежащими принудительному исполнению и юридически обязывающими (Staunton & De Stadler, 2019). Это ключевой аспект в решении уникальных проблем цифровой эпохи, когда физическое присутствие человека не является обязательным для коммерческих сделок.

Положения ECTA соответствуют меняющейся динамике современного бизнеса. Упор на правовую определенность гарантирует, что стороны, участвующие в электронных транзакциях, имеют четкое представление о своих правах, обязанностях и правовых последствиях своих действий. Эта правовая четкость способствует укреплению доверия и уверенности при взаимодействии в Интернете, снижая неопределенность, которая в противном случае может препятствовать развитию электронной коммерции и цифровых сделок.

Кроме того, принятие ECTA отражает стремление Южной Африки привести свою законодательную базу в соответствие с международными нормами. В условиях ускоряющейся глобализации гармонизация правовых принципов, связанных с электронными сделками, способствует развитию трансграничной коммерции и международных торговых отношений.

Введение в действие ECTA свидетельствует не только об адаптивности правовой базы, но и о ее устойчивости в условиях стремительного развития цифровых технологий. Рассматривая все сложности электронных взаимодействий и сделок, закон закладывает основу для создания надежной системы, способствующей дальнейшему развитию электронной коммерции при соблюдении правовых принципов.

Закон об электронных коммуникациях и сделках является значимым ответом на цифровую трансформацию коммерции, воплощая в себе проактивный подход Южно-Африканской Республики к реформированию своей правовой базы. Благодаря признанию электронных подписей, контрактов и коммуникаций ECTA восполняет пробел между традиционными правовыми нормами и непрерывно изменяющимся цифровым ландшафтом, способствуя правовой определенности и доверию при электронных взаимодействиях.

5. Интеллектуальная собственность и цифровые инновации

Конвергенция цифровых технологий и прав интеллектуальной собственности привела к необходимости пересмотреть законы об авторском праве, патентах и товарных знаках. Так, например, Поправка об авторском праве (Copyright Amendment) решает проблемы, связанные с цифровым воспроизведением и распространением творческих произведений. Способствуя достижению баланса между интересами авторов, инноваторов и широкой общественности, закон направлен на стимулирование цифровых инноваций при сохранении прав интеллектуальной собственности.

Слияние цифровых технологий и сферы интеллектуальной собственности привело к фундаментальной переоценке существующих правовых основ, включая законы об авторском праве, патентах и товарных знаках. Поскольку цифровые платформы играют ведущую роль в создании, распространении и использовании творческих работ и инновационных идей, южноафриканская система законодательства начала реформы с целью приведения защиты интеллектуальной собственности в соответствие с уникальной динамикой цифровой эпохи.

Одним из ярких примеров такого реформирования является принятие Поправки об авторском праве. Признавая проблемы, возникающие в связи с цифровым воспроизведением и распространением творческих работ, этот закон тем самым признает и сложности взаимодействия между цифровыми технологиями и охраной авторских прав (Dove & Chen, 2020). При этом сделана попытка решить проблемы, связанные с несанкционированным тиражированием и распространением цифрового контента, и установить механизмы, препятствующие нарушению прав авторов в цифровой сфере.

Центральное место в законе занимает попытка найти тонкий баланс между конкурирующими интересами авторов, инноваторов и широкой общественности. Расширяя сферу действия положений о добросовестном использовании, данный закон позволяет трансформировать использование объектов, охраняемых авторским правом, и тем самым способствует развитию цифровых инноваций и творчества. Таким образом, в законе воплощено понимание того, что традиционная парадигма авторского права требует адаптации к новым способам использования и создания контента, которые стали возможны благодаря цифровым технологиям.

Помимо авторского права, изменения коснулись и патентного законодательства, и законодательства о товарных знаках, поскольку цифровые инновации часто выходят за рамки традиционных границ. Например, рост числа патентов на программное обеспечение и бизнес-методы привел к появлению ряда правовых положений, которые ставят под сомнение традиционные патентные доктрины (Talkmore, 2022). Аналогичным образом эволюционирование цифровых товарных знаков требует пересмотра процессов их регистрации и защиты онлайн-брендов в условиях глобализации цифрового ландшафта.

По сути, изменения в законодательстве в области интеллектуальной собственности являются примером активного реагирования Южно-Африканской Республики на динамичное взаимодействие цифровых технологий и способов творческого самовыражения. Законодательные изменения, воплощенные в Законе о внесении поправок в законодательство об авторском праве, подчеркивают стремление страны создать благоприятную среду для цифровых инноваций и творчества, обеспечивая при этом защиту прав создателей контента и инноваторов.

Кроме того, конвергенция цифровых технологий и прав интеллектуальной собственности требует комплексных правовых реформ, позволяющих ориентироваться в сложных областях творчества, инноваций и цифровых достижений. Решая проблемы, возникающие в связи с цифровым воспроизведением, распространением и преобразованием продуктов творчества, южноафриканское законодательство стремится создать экосистему, стимулирующую цифровые инновации и сохраняющую неприкосновенность прав интеллектуальной собственности.

6. Проблемы юрисдикции и правоприменения

Поскольку цифровые технологии не имеют географических границ, южноафриканское законодательство столкнулось с юрисдикционными проблемами при борьбе с транснациональными цифровыми преступлениями. Для обеспечения эффективной борьбы с киберпреступниками, действующими в иностранных юрисдикциях, необходимо международное сотрудничество, договоры об экстрадиции, а также тонкий подход к сбору и сохранению цифровых доказательств.

В условиях все более взаимосвязанного мира, движимого цифровыми технологиями, южноафриканское законодательство сталкивается со сложным набором юрисдикционных и правоприменительных проблем при борьбе с транснациональными цифровыми преступлениями. Поскольку деятельность киберпреступников с легкостью преодолевает географические границы, ограничения традиционных правовых рамок становятся очевидными, что требует адаптивного реагирования на меняющуюся природу цифровой преступности.

В условиях общего цифрового ландшафта киберпреступники используют уязвимости независимо от расстояний, нанося значительный ущерб в разных юрисдикциях (Van Niekerk, 2018). В связи с этим возникают серьезные проблемы с юрисдикцией, поскольку правоохранительные органы ЮАР вынуждены преследовать преступников за пределами своих национальных границ.

Выход из этого затруднительного положения лежит в плоскости международного сотрудничества. Обеспечение эффективного применения южноафриканского законодательства в отношении киберпреступников, действующих в иностранных юрисдикциях, зависит от установления прочных партнерских отношений с другими странами. Договоры об экстрадиции играют ключевую роль в обеспечении возможности преследования и выдачи киберпреступников, которые должны понести наказание в рамках южноафриканской правовой системы. Такие договоры обеспечивают необходимую правовую основу для преодоления юрисдикционных барьеров, препятствующих уголовному преследованию транснациональных преступлений в сфере цифровых технологий.

Центральной проблемой правоприменения являются сбор и сохранение цифровых доказательств. Цифровые доказательства по своей природе нестабильны и легко поддаются манипулированию, что требует тщательного и технологически обоснованного подхода к обеспечению их целостности и допустимости в судебном процессе. При этом необходимо глубоко понимать методы сохранения данных, законы о конфиденциальности данных и международные протоколы, гарантирующие легитимность представленных в суд доказательств.

Кроме того, применение южноафриканского законодательства в сфере транснациональных цифровых преступлений требует всестороннего понимания международных правовых инструментов, таких как Будапештская конвенция о киберпреступности. Эта конвенция служит основой для международного сотрудничества в области расследования и преследования киберпреступлений, подчеркивая важность гармонизации правовых подходов разных стран[5].

Сфера транснациональных цифровых преступлений ставит перед южноафриканским законодательством многогранные задачи в области юрисдикции и правоприменения. Поскольку действие цифровых технологий не зависит от географических границ, для эффективного реагирования требуется международное сотрудничество, в частности, договоры об экстрадиции (Dove & Chen, 2020) и эффективные методы сбора доказательств. Проводимые реформы в правоприменительной практике подчеркивают необходимость решения проблемы киберпреступности, освоения сложных нюансов международного права и работы с цифровыми доказательствами.

7. Развитие юридических процедур

Развитие цифровых технологий привело также к изменениям традиционных юридических процедур. В настоящее время суды решают вопросы, связанные с цифровыми доказательствами, расследованием с использованием электронных средств и ИИ. При разрешении споров с целью ускорения процесса используются онлайн-платформы. Необходимо учитывать непрерывно меняющуюся динамику цифрового взаимодействия.

---

5 Council of Europe. (2001). Convention on Cybercrime. https://clck.ru/36cr32

Интеграция цифровых технологий в различные аспекты жизни общества стала катализатором глубоких изменений в традиционных правовых процессах. По мере адаптации правового ландшафта к требованиям цифровой эпохи южноафриканские суды оказываются на перекрестке инноваций, решая многогранные задачи и используя возможности, возникающие в связи с внедрением технологий в судопроизводство.

Одним из заметных аспектов этой трансформации является обращение с цифровыми доказательствами. Распространение цифрового взаимодействия потребовало процессов переоценки сбора, сохранения и представления доказательств. Теперь перед судами стоит задача разобраться в тонкостях цифровой криминалистики и обеспечить целостность и допустимость электронных доказательств, соблюдая при этом принципы надлежащей правовой процедуры (Swales, 2018). Это подразумевает соблюдение тонкого баланса между эффективностью технологий и обеспечением справедливости судопроизводства.

Электронные методы расследования, называемые также e-discovery, стали краеугольным камнем современного судебного процесса. Оцифровка огромных массивов данных требует применения эффективных и систематических методов выявления, сбора и представления доказательств. Это новшество побуждает юристов использовать технологические инструменты и платформы, которые способствуют эффективному управлению цифровыми доказательствами и рационализации процесса расследования.

Кроме того, использование искусственного интеллекта в юридических исследованиях вносит трансформационный аспект в юридическую науку и процесс принятия решений. Алгоритмы ИИ служат для анализа огромных массивов данных, ускоряя проведение расследования, обзоров прецедентов и судебной практики. Использование искусственного интеллекта ускоряет поиск информации, дает более точные правовые обоснования и юридические аргументы.

Цифровизация юридических процедур также привела к появлению онлайн-платформ для урегулирования споров (online dispute resolution, ODR). В них цифровые технологии используются для реализации эффективных и общедоступных механизмов разрешения споров (Kahungi, 2022). Такие платформы учитывают меняющуюся динамику цифрового взаимодействия, позволяя сторонам участвовать в процессах урегулирования без ограничений, связанных с физическим присутствием. Тем самым достигается ускорение процесса разрешения споров с учетом реалий современной коммуникации.

Интеграция цифровых технологий в традиционные юридические процессы свидетельствует о динамичной эволюции правового ландшафта. Суды, юристы и тяжущиеся стороны сталкиваются с необходимостью взаимодействовать с проблемами и возможностями, которые предоставляют такие феномены, как цифровые доказательства, электронное расследование, исследования на основе искусственного интеллекта и урегулирование споров в режиме онлайн. По мере адаптации юридических процессов к цифровой эпохе реализуется потенциал повышения эффективности и расширения доступа к правосудию в Южно-Африканской Республике, что сочетается с необходимостью обеспечения надлежащей правовой процедуры и сохранения законных прав граждан.

Заключение

Подводя итоги, можно сказать, что сложный процесс адаптации южноафриканского законодательства к стремительному развитию цифровых технологий представляет собой непрерывное взаимодействие, в ходе которого достигается хрупкое равновесие между развитием технологий и сохранением фундаментальных прав и коллективных интересов отдельных граждан и общества в целом. Этот адаптивный путь в правовом поле отражает сознательные усилия по гармонизации постоянно развивающейся цифровой сферы с устоявшимися правовыми принципами, представляя собой динамичное взаимодействие, формирующее контуры правовой системы страны.

Изменчивость развивающейся правовой базы подчеркивает стремление страны обеспечить гармоничное сочетание интеграции цифровых технологий с общественными ценностями и правами человека. Это стремление находит свое выражение в многогранном подходе, согласно которому различные отрасли права были реформированы для решения новых задач, возникающих в цифровую эпоху. Многообразные компоненты этой гибкой правовой архитектуры представлены такими ключевыми областями, как защита данных, законодательство о киберпреступности, электронные сделки, интеллектуальная собственность и юрисдикционные вопросы.

Первостепенной задачей комплексных инициатив по защите данных остается уважение к частной жизни и личной автономии человека в цифровую эпоху (Bester, 2023). Введение жестких норм обеспечивает ответственное обращение с гигантскими объемами персональных данных, используемых в сфере цифровых технологий, и защиту прав граждан даже в условиях стремительного развития инноваций, основанных на использовании данных. В то же время принятие законодательства о киберпреступности отражает активную позицию по защите цифровой сферы от недобросовестных действий, тем самым способствуя сохранению как технологической экосистемы, так и интересов граждан (Bester, 2023).

Законодательное регулирование электронных транзакций свидетельствует о стремлении ЮАР создать процветающую цифровую экономику. Удостоверяя электронные подписи, контракты и акты коммуникации, закон стимулирует предпринимателей полнее использовать потенциал электронной коммерции, способствуя тем самым экономическому росту и обеспечивая законность и правомерность цифровых сделок.

Кроме того, реформирование законодательства в области интеллектуальной собственности подчеркивает понимание тонкой взаимосвязи между творчеством, инновациями и техническим прогрессом. Уравновешивая интересы авторов, инноваторов и широкой общественности, эти изменения способствуют созданию благоприятной среды как для цифровых инноваций, так и для защиты прав интеллектуальной собственности, отражая глубокое понимание двойственной природы прогресса и сохранения традиционных ценностей.

Не менее важны и изменения в области юрисдикции, касающиеся географически неограниченного характера цифровых операций. Реагирование правовой системы на трансграничные киберпреступления свидетельствует о ее стремлении преодолеть вызовы, порождаемые глобальным взаимодействием и необходимостью отправления правосудия в коммерческой сфере, лишенной привычных географических ограничений.

Такой адаптивный правовой подход свидетельствует о стремлении органично вписать правовой ландшафт в цифровую эпоху, сохранив его актуальность и эффективность. При этом по мере развития цифровых технологий появляются новые вызовы и возможности. Поэтому адаптация южноафриканского законодательства к новым условиям остается постоянной задачей, требующей неусыпной бдительности. Правовая система готова реагировать на возникающие сложности и преобразования, обеспечивая защиту прав, чаяний и благосостояния населения страны и его развития в условиях непрерывной эволюции цифрового ландшафта.

По существу, адаптация южноафриканского законодательства к цифровым технологиям – это не цель, а динамичный процесс, постоянное стремление привести правовые нормы страны в соответствие с непрерывно меняющимися контурами цифровой эпохи. По мере расширения границ технологических инноваций адаптационные способности правовой системы будут играть все более важную роль в управлении этим процессом, определяя гармонию инноваций, правосудия и общественного благополучия.

Список литературы

Adams, R., & Adeleke, F. (2020). Protecting information rights in South Africa: the strategic oversight roles of the South African Human Rights Commission and the Information Regulator. *International Data Privacy Law*, *10*(2), 146–159. https://doi.org/10.1093/idpl/ipz022

Botha, J., Grobler, M., Hahn, J., & Eloff, M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. https://goo.su/e5JBlq

Bester, K. J. (2023). *Exploring the views and perceptions of cybersecurity among south african military officers*. https://goo.su/r7BU4

Bronstein, V. (2022). Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal*, *25*, 1–41. https://doi.org/10.17159/1727-3781/2022/v25i0a11661

Burchell, J. (2009). 'The legal protection of privacy in South Africa: A transplantable hybrid'. *Electronic Journal of Comparative Law (EJCL)*, *13*(1) 1–26. https://clck.ru/36csJ3

de Bruyn, M. (2014). The Protection of Personal Information (POPI) Act – Impact on South Africa. *International Business & Economics Research Journal (IBER)*, *13*(6), 1315–1340. https://doi.org/10.19030/iber.v13i6.8922

De Sousa, W. G., Fidelis, R. A., De Souza Bermejo, P. H., Da Silva Gonçalo, A. G., & De Souza Melo, B. (2021). Artificial intelligence and speedy trial in the judiciary: Myth, reality or need? A case study in the Brazilian Supreme Court (STF). *Government Information Quarterly*, *39*(1), 101660. https://doi.org/10.1016/j.giq.2021.101660

Dove, E. S., & Chen, J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law*, *10*(2), 117–131. https://doi.org/10.1093/idpl/ipz023

Kahungi, N. (2022). Dawn of Artificial Intelligence in Alternative Dispute Resolution; Expanding Access to Justice through Technology. *University of Nairobi Law Journal*, *2*(2). https://clck.ru/36csLM

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

Mokofe, W. M., & van Eck, S. (2021). Reflections on Marginalised Workers and the Role of Trade Unions in the Changing World of Work. *Industrial Law Journal*, *41*(3), 1365–1389. https://clck.ru/36csMJ

Mokofe, W. M., & van Eck, S. (2022). COVID-19 at the workplace: What lessons are to be gained from early case law? *De Jure Law Journal*, *55*(1). https://doi.org/10.17159/2225-7160/2022/v55a10

Mtuze, S. (2022). The convergence of legislation on cybercrime and data protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 & the Protection of Personal Information Act 4 of 2013. *Obiter*, *43*(3), 536–569. https://doi.org/10.17159/obiter.v43i3.14883

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments. *Journal of Contemporary Roman-Dutch Law*, *79*, 51–68. https://clck.ru/36csPA

Roos, A. (2020). The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. *Comparative and International Law Journal of Southern Africa*, *53*(3), 37. https://doi.org/10.25159/2522-3062/7985

Staunton, C., & De Stadler, E. (2019). Protection of Personal Information Act No. 4 of 2013: Implications for biobanks. *South Africa Medical Journal*, *109*(4), 232–234. https://doi.org/10.7196/samj.2019.v109i4.13617

Swales, L. (2018). An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One. *Potchefstroom Electronic Law Journal*, *21*, 1–30. https://doi.org/10.17159/1727-3781/2018/v21i0a2916

Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science*, 117(7/8). https://doi.org/10.17159/sajs.2021/10808

Swales, L. (2022). The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock? *Potchefstroom Electronic Law Journal*, 25, 1–32. https://doi.org/10.17159/1727-3781/2022/v25i0a11180

Talkmore, C. (2022). The role of intellectual property rights' protection in advancing development in South Africa. *Law, Democracy and Development*, *26*,168189. https://doi.org/0.17159/2077-4907/2021/ldd.v26.7

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B. (2018). The Cybersecurity Dilemma: considerations for investigations in the Dark Web. *African Journal of Criminology & Victimology*, *31*(3), 132148. https://clck.ru/36csS9

Информация об авторе

Мокофе Уильям Манга, PhD в области права, адвокат Верховного Суда Южно-Африканской Республики
Адрес: Южно-Африканская Республика, г. Ист-Лондон, Стюарт Драйв Береа, 12
E-mail: william.mokofe@gmail.com
ORCID iD: https://orcid.org/0000-0002-5170-1304
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=h_w4XXAAAAAJ

Конфликт интересов

Автор сообщает 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: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 22 августа 2023 г.
Дата одобрения после рецензирования – 11 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.47

Digital Transformations of the South African Legal Landscape

William Manga Mokofe

High Court of South Africa
East London, South Africa

Keywords

artificial intelligence,
cybercrime,
digital technologies,
intellectual property right,
judicial practice,
law,
legislation,
online dispute resolution,
personal data protection,
South Africa

Abstract

Objective: South Africa is a country with great potential for intensive development due to the active growth and adoption of digital technologies. The rapidly emerging digital landscape is transforming the legal framework, which in turn influences the digital environment. This transformative relationship determined the focus of the research, which is to identify the legal system adaptability under dynamic changes, as well as the legal landscape evolution under digitalization and technological progress.

Methods: the study of the changing legal landscape required an interdisciplinary approach that combines legal analysis with ideas from sociology, economics, etc. In doing so, the formal-legal method was used to examine the key legal instruments shaping South Africa's digital environment and providing the opportunities and challenges of the interaction between digital technologies and South African law.

Results: the paper provides insights into how the South African legal system is addressing digital challenges; assesses the integration of digital innovations into the legal system; highlights the transformative impact of digital technologies on traditional legal processes, including collecting evidence, dispute resolution and access to justice. Finally, it evaluates the role of digital technologies in making legal processes more efficient.

Scientific novelty: the study contributes to the ongoing debate on the complex relationship between digital technologies and South African law. It shows how South African law is coping with digital complexities

and substantiates new insights into the transformation of the traditional legal paradigm as a result of digitalization, as well as its implications for legal proceedings and access to justice. By delving into the adaptations, challenges and innovations arising at the intersection of law, technologies and digitalization, insights are gained into how South African law navigates the dynamic digital landscape.

Practical significance: adapting the legal landscape to digitalization and technological advances is critical to ensure rapid technological progress. It also requires collaboration between government agencies, civil society, experts in law and technology. The study provides valuable recommendations and suggestions for policymakers, legal practitioners and stakeholders shaping South Africa's legal ecosystem. The author addresses the challenges of ensuring personal data privacy, enhancing electronic interactions, and countering cybercrime. The importance of introducing technological achievements while maintaining robust legal safeguards is emphasized.

For citation

Mokofe, W. M. (2023). Digital Transformations of the South African Legal Landscape. *Journal of Digital Technologies and Law, 1*(4), 1087–1104. https://doi.org/10.21202/jdtl.2023.47

References

Adams, R., & Adeleke, F. (2020). Protecting information rights in South Africa: the strategic oversight roles of the South African Human Rights Commission and the Information Regulator. *International Data Privacy Law*, *10*(2), 146–159. https://doi.org/10.1093/idpl/ipz022

Botha, J., Grobler, M., Hahn, J., & Eloff, M. (2017). A High-Level Comparison between the South African Protection of Personal Information Act and International Data Protection Laws. In *The 12th International Conference on Cyber Warfare and Security (ICCWS)*. https://goo.su/e5JBlq

Bester, K. J. (2023). *Exploring the views and perceptions of cybersecurity among south african military officers*. https://goo.su/r7BU4

Bronstein, V. (2022). Prioritising Command-and-Control Over Collaborative Governance: The Role of the Information Regulator Under the Protection of Personal Information Act. *Potchefstroom Electronic Law Journal*, *25*, 1–41. https://doi.org/10.17159/1727-3781/2022/v25i0a11661

Burchell, J. (2009). 'The legal protection of privacy in South Africa: A transplantable hybrid'. *Electronic Journal of Comparative Law (EJCL)*, *13*(1) 1–26. https://clck.ru/36csJ3

de Bruyn, M. (2014). The Protection of Personal Information (POPI) Act – Impact on South Africa. *International Business & Economics Research Journal (IBER)*, *13*(6), 1315–1340. https://doi.org/10.19030/iber.v13i6.8922

De Sousa, W. G., Fidelis, R. A., De Souza Bermejo, P. H., Da Silva Gonçalo, A. G., & De Souza Melo, B. (2021). Artificial intelligence and speedy trial in the judiciary: Myth, reality or need? A case study in the Brazilian Supreme Court (STF). *Government Information Quarterly*, *39*(1), 101660. https://doi.org/10.1016/j.giq.2021.101660

Dove, E. S., & Chen, J. (2020). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law*, *10*(2), 117–131. https://doi.org/10.1093/idpl/ipz023

Kahungi, N. (2022). Dawn of Artificial Intelligence in Alternative Dispute Resolution; Expanding Access to Justice through Technology. *University of Nairobi Law Journal*, *2*(2). https://clck.ru/36csLM

Malgieri, G., & Comandé, G. (2017). Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation. *International Data Privacy Law*, *7*(4), 243–265. https://doi.org/10.1093/idpl/ipx019

Mokofe, W. M., & van Eck, S. (2021). Reflections on Marginalised Workers and the Role of Trade Unions in the Changing World of Work. *Industrial Law Journal*, *41*(3), 1365–1389. https://clck.ru/36csMJ

Mokofe, W. M., & van Eck, S. (2022). COVID-19 at the workplace: What lessons are to be gained from early case law? *De Jure Law Journal*, *55*(1). https://doi.org/10.17159/2225-7160/2022/v55a10

Mtuze, S. (2022). The convergence of legislation on cybercrime and data protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 & the Protection of Personal Information Act 4 of 2013. *Obiter*, *43*(3), 536–569. https://doi.org/10.17159/obiter.v43i3.14883

Naude, A., & Papadopoulos, S. (2016). Data Protection in South Africa: The Protection of Personal Information Act 4 of 2013 in Light of Recent International Developments. *Journal of Contemporary Roman-Dutch Law*, *79*, 51–68. https://clck.ru/36csPA

Roos, A. (2020). The European Union's General Data Protection Regulation (GDPR) and its Implications for South African Data Privacy Law: An Evaluation of Selected 'Content Principles'. *Comparative and International Law Journal of Southern Africa*, *53*(3), 37. https://doi.org/10.25159/2522-3062/7985

Staunton, C., & De Stadler, E. (2019). Protection of Personal Information Act No. 4 of 2013: Implications for biobanks. *South Africa Medical Journal*, *109*(4), 232–234. https://doi.org/10.7196/samj.2019.v109i4.13617

Swales, L. (2018). An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One. *Potchefstroom Electronic Law Journal*, *21*, 1–30. https://doi.org/10.17159/1727-3781/2018/v21i0a2916

Swales, L. (2021). The Protection of Personal Information Act and data de-identification. *South African Journal of Science*, 117(7/8). https://doi.org/10.17159/sajs.2021/10808

Swales, L. (2022). The Protection of Personal Information Act 4 of 2013 in the Context of Health Research: Enabler of Privacy Rights or Roadblock? *Potchefstroom Electronic Law Journal*, 25, 1–32. https://doi.org/10.17159/1727-3781/2022/v25i0a11180

Talkmore, C. (2022). The role of intellectual property rights' protection in advancing development in South Africa. *Law, Democracy and Development*, *26*,168189. https://doi.org/10.17159/2077-4907/2021/ldd.v26.7

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication (AJIC)*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Van Niekerk, B. (2018). The Cybersecurity Dilemma: considerations for investigations in the Dark Web. *African Journal of Criminology & Victimology*, *31*(3), 132148. https://clck.ru/36csS9

Author information

William Manga Mokofe – PhD (Law), Advocate of the High Court of South Africa
Address: 12 Stewart Drive Berea, East London, South Africa
E-mail: william.mokofe@gmail.com
ORCID iD: https://orcid.org/0000-0002-5170-1304
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=h_w4XXAAAAAJ

Conflict of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
ASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 22, 2023
Date of approval – October 11, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023

Научная статья
УДК 34:004:341.492:343.11
EDN: https://elibrary.ru/zxufeq
DOI: https://doi.org/10.21202/jdtl.2023.48

Эффективность отправления правосудия в Нигерии в условиях развития цифровых технологий

Пол А. Айдоноджи ✉

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Самину А. Вакили

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Давид Аюба

Государственный университет Эдо-Узайруэ
г. Иямхо, Нигерия

Ключевые слова

виртуализация судопроизводства,
онлайн-разрешение споров,
онлайн-судопроизводство,
отправление правосудия,
право,
суд,
цифровая платформа,
цифровые технологии,
электронное делопроизводство,
электронное правосудие

Аннотация

Цель: традиционная нигерийская судебная система долгое время ассоциировалась с ее консервативным подходом и традиционными методологиями отправления правосудия. В результате развития цифровых технологий Нигерия как развивающаяся страна получила огромные преимущества, особенно в правовой сфере. Это связано с тем, что для эффективного отправления правосудия в судопроизводство Нигерии стремительно внедряются современные цифровые технологии. Однако, несмотря на перспективы развития цифровых технологий, в Нигерии существуют правовые и социально-экономические проблемы, которые могут повлиять на успешное их использование в судопроизводстве. Этим обосновывается нацеленность исследования на выявление правовых и социально-экономических проблем цифровизации судопроизводства в Нигерии.

Методы: исследование сочетает в себе доктринальный и недоктринальный подходы. Первый позволяет теоретически осмыслить концептуальные вопросы и перспективы развития виртуализации

✉ Контактное лицо

судопроизводства, изучить на основе первичных и вторичных источников (законов, монографий, научных статей и интернет-ресурсов) правовые и социально-экономические проблемы использования цифровых технологий в судопроизводстве. Второй направлен на анкетирование, описание и анализ результатов социологического опроса, проведенного среди респондентов, проживающих в Нигерии, на предмет их отношения к нововведениям в области цифровизации и виртуализации судопроизводства, а также к возникающим в связи с цифровизацией проблемам.

Результаты: исследование показало, что использование цифровых технологий в судопроизводстве Нигерии имеет ряд перспектив, обеспечивающих эффективное отправление правосудия и обеспечение точного учета и хранения данных о судебных заседаниях. Наряду с преимуществами показаны проблемы, которые могут повлиять на эффективность цифровизации судопроизводства.

Научная новизна: заключается в исследовании использования цифровых технологий в судопроизводстве Нигерии, в выявлении перспективы повышения эффективности отправления нигерийского правосудия в условиях развития цифровых технологий, а также в обусловленных этой тенденцией проблем.

Практическая значимость: исследование позволит заинтересованным сторонам нигерийского юридического сектора выявить правовые и социально-экономические проблемы, которые могут негативно повлиять на использование цифровых технологий в судопроизводстве и сделать их неэффективными. Кроме того, в статье предлагаются конкретные (практические) рекомендации по устранению этих проблем.

Для цитирования

Айдоноджи, П. А., Вакили, С. А., Аюба, Д. (2023). Эффективность отправления правосудия в Нигерии в условиях развития цифровых технологий. *Journal of Digital Technologies and Law*, *1*(4), 1105–1131. https://doi.org/10.21202/jdtl.2023.48

Содержание

Введение

Цифровые технологии стали важным инструментом для юристов, способствуя развитию и укреплению судебной системы во всем мире за счет эффективного и быстрого доступа к информации при отправлении правосудия (Meredith et al., 2021). В развитых странах технологический прогресс заметно усовершенствовал и ускорил судебные процедуры (Machado et al., 2018). Это связано с тем, что в большинстве этих развитых стран цифровые технологии широко и эффективно используются в судопроизводстве. Однако традиционная судебная система Нигерии всегда отличалась консервативным подходом, приверженностью традиционным методам отправления правосудия (Olubukola & Abimbola, 2022). Со временем такая ситуация начала негативно сказываться на состоянии судебной системы Нигерии, чему способствовало также большое количество дел, поступающих в суды, и другие социально-экономические проблемы, влияющие на отправление правосудия (Olubukola & Abimbola, 2022). В этой связи достаточно констатировать, что в свете постоянно развивающихся во всем мире технологий назрела настоятельная необходимость в повышении эффективности и результативности судопроизводства в Нигерии. Следовательно, актуальной становится задача интегрировать виртуальное судопроизводство в судебную систему Нигерии, чтобы открыть доступ к электронному управлению делами и судебным процессам.

Чтобы преодолеть существующие проблемы судопроизводства в Нигерии, Национальный судебный совет и генеральный прокурор Федерации Абубакар Малами издали директиву, согласно которой суды должны осуществлять виртуальное судопроизводство в цифровом формате (Olubukola & Abimbola, 2022). Исходя из этих указаний, некоторые штаты, такие как Лагос, Абуджа и Риверс, прибегли к дистанционному судопроизводству. Например, штат Лагос принял «Практическое указание о дистанционном рассмотрении дел в судебной системе штата Лагос», которое вступило в силу 4 мая 2020 г. (Mohamad & Sule, 2021). Целью принятия практических указаний, обеспечивающих возможность проведения виртуальных слушаний в цифровом формате, является рассмотрение несрочных и не ограниченных по времени дел с использованием платформ видео- или аудиоконференций, таких как Zoom, Skype, Google Meet или любых других, которые могут быть одобрены судом

(Mohamad & Sule, 2021). Первым штатом, где решение по уголовному делу было вынесено в режиме онлайн, стал штат Борно.

В современном мире, где технологии проникают во все сферы деятельности (Granot et al., 2018; Goethe et al., 2021), польза этой инновации не вызывает сомнений, особенно в ситуации насущной необходимости ее использования. Вместе с тем ее конституционность стала предметом споров в Нигерии (Tait & Tay, 2019). Некоторые специалисты утверждают, что действующее положение Конституции, требующее проведения публичных судебных процессов, хотя и с некоторыми исключениями, не получило полного выражения, как это указано в разделах 36(1), (3) и (4) Конституции Федеративной Республики Нигерия 1999 г. с поправками. Высказывается мнение, что до тех пор, пока в конституцию не будут внесены изменения, виртуальное судопроизводство не может применяться в нигерийских судах (Thornburg, 2021). Сторонники цифрового виртуального судопроизводства, напротив, утверждают, что для введения в действие виртуального судопроизводства в Нигерии нет необходимости вносить изменения в Конституцию, что обосновывается положениями той же Конституции (Winter et al., 2018).

В связи с вышесказанным наше исследование посвящено доктринальному и недоктринальному изучению перспектив цифрового виртуального судопроизводства в нигерийских судах. В работе также будут подробно рассмотрены правовые вопросы, связанные с цифровым виртуальным судопроизводством в нигерийских судах. Далее мы рассмотрим возможные проблемы, связанные с использованием технологий в судебных заседаниях в Нигерии, и дадим ряд рекомендаций по устранению выявленных проблем.

Методология. С учетом актуальности данной темы был принят гибридный подход, состоящий из доктринального и недоктринального методов исследования. Суть доктринального метода заключается в том, что он позволяет исследователю теоретически осмыслить концептуальные вопросы и развитие виртуального судопроизводства, а также изучить правовые и социально-экономические проблемы цифрового виртуального судопроизводства. В работе были использованы первичные и достоверные вспомогательные источники, такие как законы, сборники, статьи из научных журналов и Интернета.

Недоктринальный метод исследования позволяет изучить респондентов – граждан Нигерии – на предмет перспектив и проблем цифрового виртуального судопроизводства. С этой целью была составлена с использованием Google-формы и распространена среди различных категорий населения анкета. Полученные данные анализировались с помощью описательного и аналитического методов.

1. Концептуальная природа цифрового виртуального судопроизводства в Нигерии

В различных исследованиях подчеркивается, что судебная система Нигерии ограничена традиционными рамками (Mohamad & Sule, 2021). Эти рамки включают кабинеты адвокатов и залы суда, конференц-залы и юридические библиотеки, заполненные печатными источниками (Bannon & Keith, 2021; Bandes & Feigenson, 2021). Кроме того, неотъемлемой частью традиционной структуры являются административные помощники и другой вспомогательный персонал. К сожалению, традиционный подход приводит к увеличению количества нерассмотренных дел, затягиванию процессов

их разрешения и проблемам с доступом к эффективному правосудию (Sanson et al., 2020). Обеспечение доступа общественности к судебным процессам и защита основных свобод, предусмотренных национальным законодательством и международными соглашениями, стали одной из важнейших задач судебной системы Нигерии. В этой связи достаточно констатировать, что, хотя физическое судопроизводство имеет свои преимущества, оно также сопряжено с определенными проблемами, которые заключаются в следующем:

1. Обширная география Нигерии создает трудности для физического доступа к залам судебных заседаний, особенно в сельских и отдаленных районах. Это ограничивает доступ к правосудию и непропорционально ущемляет маргинальные слои населения.

2. Судебная система Нигерии перегружена большим количеством дел, что приводит к низкой эффективности судов и значительным задержкам в отправлении правосудия.

3. Физическое присутствие на судебных заседаниях может быть финансово обременительным для многих людей, поскольку связано с расходами на транспорт, проживанием и отрывом от работы.

4. Кроме того, в некоторых случаях физическое присутствие сторон, участвующих в судебном процессе, может быть сопряжено с риском для безопасности, запугиванием или принуждением.

Однако в развитых странах технический прогресс заметно усовершенствовал и ускорил судебные процедуры (Rossner, 2021). Учитывая сложности, часто возникающие при физическом судопроизводстве в Нигерии, можно отметить постепенное развитие технологий, связанных с оказанием юридических услуг. В связи с этим интеграция виртуального судопроизводства в судебную систему Нигерии стала настоятельной необходимостью, так как она открывает путь к расширению доступа к электронному ведению дел и проведению судебных заседаний.

В связи с вышесказанным термин «цифровое виртуальное судопроизводство», используемый в Нигерии, означает судебные заседания, проводимые в режиме онлайн, в которых участвуют судьи, юридические представители, сотрудники суда, свидетели, сотрудники службы безопасности и другие заинтересованные стороны с помощью цифровых платформ или средств связи, таких как Zoom, Google meeting, Skype и аналогичных компьютерных/интернет-устройств (Nir & Musial, 2022). В данном контексте «цифровые виртуальные технологии» означают искусственную или созданную компьютером реальность в отличие от физической реальности. Кроме того, под «заседанием в Zoom, Skype или Google» понимается цифровая виртуальная или видеоконференция. Участники могут присоединиться к таким встречам посредством веб-камер или телефонов (Derksen et al., 2020). «Переговорная комната Zoom, Skype или Google» – это среда, позволяющая людям инициировать встречи онлайн, проводить удаленную работу и взаимодействие (Legg & Song, 2021). Аналогичным образом унифицированные коммуникационные платформы объединяют различные каналы деловой коммуникации, такие как онлайн-встречи, обмен мгновенными сообщениями, видеоконференции и т. д. (Hwang et al., 2021).

В этой связи необходимо отметить, что цифровое виртуальное судопроизводство в нигерийских судах предполагает использование цифровых платформ для проведения таких юридических действий, как слушания и судебные процессы (Elek et al., 2012). Этот подход направлен на повышение доступности, эффективности

и удобства за счет использования технологий, позволяющих участвовать в судебных процессах дистанционно (Bandes & Feigenson, 2020), включая представление доказательств и выдвижение юридических аргументов без необходимости физического присутствия в зале суда (Bild et al., 2021). Реализация виртуального судопроизводства требует тщательной проработки технологической инфраструктуры и мер безопасности, а также обеспечения справедливости и прозрачности судебных процессов (Bandes & Feigenson, 2020).

Кроме того, виртуальные судебные слушания могут проводиться в двух формах: гибридной или полностью виртуальной (Fauville et al., 2021). При гибридном подходе одни стороны физически присутствуют в определенном месте, а другие участвуют в процессе в режиме онлайн (Feigenson, 2010). Это включает сценарии, когда судья, секретарь и свидетели физически присутствуют в открытом судебном заседании, а другие участники присоединяются к ним виртуально (Bunjavec, 2020). В другом варианте судья, секретарь и адвокаты могут присутствовать в открытом судебном заседании, а свидетели подключаются к процессу дистанционно (Bailenson, 2021). Полностью виртуальный подход предполагает участие всех сторон из разных мест, включая судью, адвокатов, свидетелей и помощников (Hans, 2022).

В связи с вышесказанным следует отметить, что внедрение цифрового виртуального судопроизводства имеет ряд перспектив, которые могут улучшить практику судопроизводства в Нигерии. В связи с этим адвокаты и лица, обращающиеся за правосудием, должны адаптироваться к изменяющимся условиям, используя цифровые технологии для улучшения отправления правосудия.

2. Перспективы развития цифрового виртуального судопроизводства в Нигерии

Виртуальное судопроизводство в Нигерии позволяет преодолеть множество проблем, связанных с обычными судебными процессами (Mohamad & Sule, 2021). Внедрение его в Нигерии вызвало бурные дискуссии, в ходе которых сторонники и противники высказывали свои точки зрения (Olubukola & Abimbola, 2022). В них подчеркивались преимущества внедрения такого судопроизводства, а также рассматривались проблемы, которые необходимо решить для его эффективного функционирования (Olubukola & Abimbola, 2022). Сторонники такого судопроизводства подчеркивают удобство и перспективы, которые оно открывает для отправления правосудия в стране (Mohamad & Sule, 2021). Среди отмеченных учеными-юристами преимуществ цифрового виртуального судопроизводства можно особо выделить следующие:

– удобство для всех сторон процесса;

– избавление от ненужных потерь времени на поездки для физического участия в судебных заседаниях;

– акцент на принципах справедливого разбирательства, предусмотренных Конституцией Нигерии;

– низкие затраты и экономическая выгода;

– избавление от проблем больших расстояний, которые могут служить барьером для отправления правосудия;

– возможность ведения точного учета и сохранения информации о судебных заседаниях;

– снижение нагрузки на судью и адвокатов при ведении протокола.

Исходя из вышесказанного, можно с уверенностью утверждать, что, несмотря на возможные недостатки, виртуальное судопроизводство – это инструмент, который должен быть принят судебной системой Нигерии, поскольку повысит ее эффективность и прозрачность, а значит, осуществит надежду широких масс на справедливое правосудие.

3. Правовая база, регулирующая виртуальное судопроизводство в Нигерии

Что касается правовых основ цифрового виртуального судопроизводства в нигерийских судах, то точнее всего ситуацию характеризует высказывание главного судьи штата Борно Кашима Заннаха в его работе под названием «Достижения в области технологий: руководство или реквием для юридической практики». По его словам, будущее нашей юридической сферы невозможно без технологий, которые будут пронизывать социально-экономическую ткань нашего общества. Далее судья пишет, что подобно тому, как вымерли динозавры, бумажная работа в юридической практике также исчезнет.

Таким образом, неоднозначная реакция на практику виртуального судопроизводства в нигерийских судах может быть устранена путем тщательного изучения положений нигерийского законодательства. Наиболее часто возникающий вопрос с момента внедрения цифровых виртуальных судебных процедур связан с законностью в рамках нигерийской правовой экосистемы. Этот вопрос проистекает из убеждения, что для всего нужна твердая основа. Поэтому некоторые правоведы не приветствуют цифровые виртуальные судебные процессы в любой форме на том основании, что нигерийское законодательство не поддерживает цифровые виртуальные процессы, а значит, любая практика такого рода является неконституционной и незаконной. Представители этой категории юристов считают, что для того, чтобы виртуальные слушания были законными в нигерийском суде, необходимо внести соответствующие поправки в Конституцию Нигерии. В то же время другие приветствуют это явление и считают его конституционным и законным. Они утверждают, что в Конституцию вносить поправки не нужно.

В связи с вышеизложенным мы рассмотрим законность цифрового виртуального судопроизводства в Нигерии и докажем, что она предусмотрена нигерийскими конституционными, законодательными и судебными органами, которые признают наличие правовой основы для цифрового виртуального судопроизводства.

3.1. Признание Конституцией Нигерии цифрового виртуального судопроизводства

Конституция Федеративной Республики Нигерия 1999 г. (с поправками) является основным законом страны, на который опираются все остальные законы. Раздел 1(3) Конституции Нигерии гласит, что любой закон, противоречащий положениям Конституции, объявляется недействительным в меру такого несоответствия. Соответствующие положения, касающиеся цифрового виртуального судопроизводства, содержатся в разделах 36(3) и (4). Эти положения Конституции устанавливают модель в отношении действительности цифрового виртуального судопроизводства в Нигерии. Раздел 36(3) Конституции Нигерии предусматривает, что

заседания суда или трибунала должны проводиться публично. Кроме того, раздел 36(4)(a) предусматривает, что лицо, обвиняемое в суде или трибунале, должно быть заслушано публично.

Если рассмотреть вышеприведенные положения Конституции Нигерии в совокупности, становится ясно, что основным требованием для признания любого судебного разбирательства действительным или его прекращения является публичное проведение такого разбирательства. Формулировки разделов 36(3) и (4) Конституции однозначно требуют публичного судебного разбирательства. В подтверждение законности цифровых виртуальных судебных заседаний следует отметить, что в Конституции Нигерии под судом никогда не понимается помещение, здание или место (в смысле физического местонахождения). Тем самым утверждается, что суд – это скорее услуга, чем общедоступное место. В этой связи необходимо констатировать, что цифровые виртуальные судебные процессы открыты для общественности, а значит, являются судебными процессами согласно Конституции Нигерии. Хотя цифровое виртуальное судопроизводство прямо не упоминается в Конституции Нигерии, оно подразумевается при толковании разделов 36(3) и (4). Комментируя понятие «публичный», используемое в разделе 36 Конституции, судья Per Muhammad JCA в деле Kosebinu & Ors V Alimi[1] высказал мнение, что для квалификации места в качестве публичного в соответствии с разделом 36(3) Конституции Федеративной Республики Нигерия от 1999 г. достаточно, чтобы оно было доступно для представителей общественности, и для этого не требовалось бы разрешения или согласия судьи. Показательным в этом отношении является дело NAB Ltd v Barri Eng. Nig. Ltd., в котором судья (Per Belgore JSC) отметил, что публичное слушание подразумевает ситуацию, когда широкая общественность не лишена доступа к нему.

В связи с вышесказанным достаточно констатировать, что Конституция, хотя и не содержит прямого указания или положения о цифровом виртуальном судопроизводстве, но косвенно допускает его, поскольку цифровая виртуальная платформа может рассматриваться как еще более открытая площадка, чем здание суда. Кроме того, согласно тривиальному юридическому принципу, подтвержденному Верховным судом Нигерии в деле Anyeabosi v. R.T Briscoe Ltd[2], то, что не запрещено, то разрешено. Кроме того, в деле Theophilus v FRN[3] суд постановил, что основной принцип или канон толкования закона гласит, что то, что прямо не запрещено законом, подразумевается разрешенным. Далее суд указал, что суд не обладает интерпретационной юрисдикцией или полномочиями толковать закон так, чтобы он означал то, что он не означает, а также толковать закон таким образом, чтобы он не означал того, что он означает. Кроме того, в деле Attorney General of Bendel State v Attorney General of the Federation[4] (судья Per Obaseki JSC) Верховный суд отметил и предупредил, что следует избегать узкого толкования Конституции.

1 (2005) LPELR 11442 (CA).

2 (1987) 3 NWLR (Pt. 59) 108; Alhaji Ibrahim Hassan & Anor v Jafar Abubakar & Ors LER (2015) SC 732/2015.

3 (2012) LPELR 9846.

4 (1981) 10 SC 1.

В деле FRN v Fani-Kayode[5] суд вновь указал на необходимость активного подхода к толкованию закона, а также на то, что суд не должен налагать на себя ограничения, не предусмотренные законом.

Таким образом, в свете приведенных выше примеров представляется, что Конституция Нигерии ни в одном из своих положений не запрещает цифровые виртуальные судебные процессы, а, скорее, подразумевает разрешение на использование цифровых технологий в судопроизводстве. Кроме того, в разделе 36(3) и (4) Конституции не упоминается какое-либо физическое помещение или здание, поэтому слово «суд» не должно ограничиваться ими. В связи с этим смысл выражения «публичное слушание», используемого в разделах 36(3) и (4) Конституции, сводится к тому, что оно является доступным для представителей общественности. Цифровое виртуальное судопроизводство отвечает этому требованию, поскольку оно доступно для общественности, и на этом основании можно утверждать, что цифровое виртуальное судопроизводство в нигерийском суде является законным и конституционным.

Более того, правовые рамки виртуального судопроизводства в нигерийском суде могут быть расширены за пределы положений разделов 36(3) и (4) Конституции и судебных органов. Это связано с тем, что в соответствии с разделами 236, 248, 254, 259, 264, 269, 274, 279 и 284 Конституции Нигерии главы и председатели различных судов могут по своему усмотрению устанавливать правила, известные как правила суда, для осуществления процедур в соответствующих судах. Так, положения раздела 274 Конституции предусматривают, что главный судья каждого из 36 нигерийских штатов должен устанавливать правила, регулирующие практику и процедуры Верховного суда в соответствующем штате. Именно в соответствии с этими полномочиями и в порядке их реализации некоторые штаты Нигерии приняли правила, позволяющие проводить виртуальные разбирательства в цифровом формате.

В связи с этим возникает вопрос, не противоречит ли практическое указание главных судей этих штатов о цифровом виртуальном судопроизводстве в их штатах положениям разделов 36(3) и (4) Конституции Нигерии, учитывая, в частности, положения раздела 274 Конституции, которые наделяют главных судей штатов правом устанавливать правила для регулирования процедур в Верховных судах штатов. Правовая позиция заключается в том, что Конституция является основным законом и имеет преимущественную силу. В соответствии с разделом 1(3) Конституции Нигерии любой закон, не соответствующий положениям Конституции, должен быть признан недействительным в той степени, в которой он не соответствует Конституции. Так, в деле Buhari v INEC[6] суд постановил, что любое практическое указание, признанное не соответствующим положениям разделов 36(3) и (4) Конституции Федеративной Республики Нигерия от 1999 г. (с поправками), должно быть признано недействительным. Но тогда является ли практическое указание, предусматривающее практику виртуального судопроизводства в нигерийском суде, несовместимым с положениями разделов 36(3) и (4) Конституции? Следует ли считать его подпадающим под требования раздела 1(3) Конституции и постановления по делу

5 (2010) 14 NWLR (Pt.1214)481 at 503.

6 (2008) 3NWLR 465.

Buhari v INEC, то есть признать его неконституционным? При ответе на этот вопрос показательным является решение Верховного суда по недавнему незарегистрированному делу Lagos State V Ekiti State Government[7]. В этом деле суд должен был определить, является ли конституционным требование о том, что судебные заседания, за некоторыми исключениями, должны проводиться публично, и являются ли конституционными судебные слушания с использованием технологий, а именно дистанционные слушания любого рода, будь то с помощью Zoom, WhatsApp, Microsoft Themes, Skype или любой другой платформы для аудиовизуальных или видеоконференций. Разрешая этот вопрос, Верховный суд назвал его несвоевременным и спекулятивным, прекратил дело и заявил, что, согласно действующему в Нигерии законодательству, цифровые виртуальные судебные процессы являются конституционными. Таким образом, была подтверждена законность цифрового виртуального судопроизводства в нигерийских судах. Это решение получило одобрение со стороны ряда известных юристов, в том числе бывшего вице-президента Нигерии профессора Йеми Осибанджо, который выступил на вебинаре, посвященном освещению в СМИ виртуального судопроизводства в Нигерии. Исследователь Силк положительно оценил это решение и заявил, что идея компьютеризации судопроизводства рассматривалась уже много лет, поэтому одобрение виртуального судопроизводства постановлением Верховного суда является логичным. По его словам, оно, помимо прочего, спасло нашу систему правосудия от очередного раунда решений судов о конституционности цифровых виртуальных судебных процедур.

Итак, мы установили, что виртуальное судопроизводство в нигерийском суде является законным и конституционным. Следует также отметить, что, помимо Конституции и судебных органов, существуют правила суда, которые предусматривают цифровое виртуальное судопроизводство в Нигерии. Для целей данного исследования особый интерес представляют правила и практические указания Национального промышленного суда Нигерии и Высокого суда штата Лагос.

3.2. Практические указания и руководства Национального промышленного суда Нигерии от 2020 г.

Указания и рекомендации по практике судопроизводства в области национальной промышленности вступили в силу 18 мая 2020 г. Руководство направлено на обеспечение быстрого рассмотрения дел и доступности правосудия. Кроме того, оно также направлено на соблюдение указаний, способствующих борьбе с коронавирусом (Covid-19). Однако в Руководстве также предусмотрена процедура, при которой судебное разбирательство осуществляется виртуально с использованием электронных устройств. Это касается всего судебного процесса – от подачи документов до вынесения решений. В этой связи раздел 4(1) Практических указаний и руководства по проведению судебных заседаний Национального промышленного суда Нигерии предусматривает подачу судебных исков в электронном виде. В нем говорится, что все документы, которые сторона хочет подать, должны быть отсканированы или преобразованы в формат PDF и направлены в секретариат суда через специально выделенный для этой цели адрес электронной почты или сервис WhatsApp. Кроме того,

[7] SC/CV/260/2020 (Unreported).

подаваемый иск должен быть подписан адвокатом и заверен печатью. Однако подраздел 2 раздела 4 Практического руководства предусматривает физические способы подачи документов в тех случаях, когда электронная подача невозможна. Раздел 4(4) Практического руководства предусматривает, что если иск подается в электронном виде, то стороны и адвокат должны указать электронную почту или телефон, по которому с ними можно связаться. Раздел 5 Практического руководства 2020 г. регулирует вопросы уплаты пошлины за подачу иска. Раздел 5(1) данного Руководства гласит, что оплата пошлины за подачу иска должна производиться в электронном виде путем перечисления средств. Кроме того, раздел 6 Практического руководства предусматривает электронный способ передачи судебных документов, а также уведомления о слушании. Разделы 6(2), (3) и (4) устанавливает, что стороны во всех подаваемых ими процессуальных документах должны указывать контактный адрес с электронной почтой или номер телефона, по которому им могут быть переданы судебные документы как сотрудниками суда, так и другой стороной. Этот контактный адрес также необходим для извещения сторон о слушании дела. В соответствии с разделом 6(6) Практического руководства передача документов считается надлежащим образом завершенной, а документы доставленными, как только электронное средство, использованное для доставки, покажет соответствующее уведомление.

Можно сказать, что наиболее значимым положением Руководства по практике судопроизводства в области национальной промышленности является раздел 7(1). В нем говорится, что цифровые виртуальные судебные заседания заменяют физические слушания в течение всего периода Covid-19, за исключением вопросов чрезвычайной важности, которые не могут быть рассмотрены судом в виртуальном режиме. Однако вопросы, подпадающие под эту категорию, должны быть перечислены и оглашены руководителями Национального промышленного суда. В разделе 7(2) говорится, что все вопросы бесспорного характера и дела, не требующие представительства или рассмотрения доказательств, относятся к категории вопросов, которые могут быть рассмотрены дистанционно. Кроме того, в соответствии с подразделом 2 все решения, постановления и указания суда должны выноситься в виртуальном режиме. Раздел 7(3) предусматривает средства или цифровые платформы, с помощью которых может осуществляться виртуальное судопроизводство. В нем прямо и конкретно упоминается видео-конференц-связь, а также оговаривается, что это может быть любое другое средство или цифровая технологическая платформа, одобренная судом. Следует отметить, что раздел 7(7) Практического руководства, как представляется, вновь подчеркивает положения разделов 36(3) и (4) Конституции Нигерии 1999 г. Это связано с тем, что, согласно данному разделу, суд должен обеспечить доступность виртуального слушания для представителей общественности, за исключением случаев, когда речь идет о частичном применении или других процедурах, которые в соответствии с действующим законодательством или правилами суда должны проводиться в кабинете судьи.

В связи с вышесказанным уместно подытожить, что практические рекомендации и руководства обусловлены положениями разделов 36(3) и (4) Конституции Нигерии. Как представляется, практические указания и рекомендации Национального промышленного суда от 2020 г. предусматривают цифровое виртуальное судопроизводство. При этом практические указания и рекомендации относятся только к Национальному промышленному суду Нигерии, а значит, все остальные суды не обязаны соблюдать и исполнять их.

3.3. Практическое руководство по дистанционному рассмотрению дел в судебной системе штата Лагос до 2029 г.

Данное Практическое руководство было составлено главным судьей штата Лагос Казимом О. Алогба. Следует отметить, что оно подготовлено в соответствии с положениями Конституции Нигерии, Закона об отправлении уголовного правосудия штата Лагос и Правил судопроизводства штата Лагос, которые уполномочивают главного судью штата устанавливать нормы, регулирующие деятельность судов в пределах юрисдикции штата. Раздел 5 Практического руководства предусматривает, что все цифровые виртуальные судебные процессы должны соответствовать положениям Конституции Нигерии и всем другим применимым законам.

Разделы 6–10 касаются подачи судебных документов и оплаты судебных издержек. В этой связи раздел 7 Практического руководства предусматривает, что документ, подаваемый в электронном виде, должен быть отсканирован или преобразован в формат PDF и передан в секретариат суда по электронной почте или через WhatsApp по номеру, предназначенному для этой цели. Однако оговорка к разделу 7 Практического руководства предусматривает, что если подача документов в электронном виде невозможна, то они могут быть поданы в секретариат суда в физическом виде. Раздел 11 предусматривает, что вручение судебных документов должно осуществляться в электронном виде по e-mail, WhatsApp или по указаниям суда, если таковые имеются. В этой связи раздел 13 также предусматривает, что если подача документов осуществляется в электронном виде, то время начинает исчисляться с момента отправки, а не с момента получения.

Для целей настоящего исследования наиболее значимыми положениями Практического руководства являются разделы 14–18. Они посвящены характеру цифрового виртуального судопроизводства, используемой платформе и другим условиям. Так, раздел 14 предусматривает, что стороны и адвокаты должны спланировать виртуальное заседание с секретариатом. В то же время в разделе 16 указаны цифровые технологические платформы, на которых могут проводиться виртуальные судебные заседания. К ним относятся Zoom, Skype или любой другой способ связи, одобренный судьей. Раздел 17, в свою очередь, предписывает сторонам и адвокатам обеспечить наличие средств, необходимых для проведения виртуального слушания в цифровом формате. Данный раздел также предусматривает, что уведомление о судебном заседании должно быть размещено на сайте судьи, а также указано в списке дел, запланированных для рассмотрения судом. Кроме того, раздел 19 устанавливает, что суд должен направлять и инструктировать стороны и адвокатов по вопросам использования видео-конференц-связи и аудиосвязи в ходе разбирательства. Раздел 20 Практического руководства также предусматривает, что адвокаты, участвующие в виртуальном заседании, должны быть одеты в соответствии с дресс-кодом, принятым в юридической профессии. Что касается записи виртуального судебного процесса в цифровом формате, то раздел 21 наделяет суд правом вести запись судебного процесса. Однако в разделе 22 оговаривается, что адвокаты сторон могут вести запись только после получения разрешения суда.

Следует отметить, что вышеприведенные положения Практического руководства штата Лагос в достаточной степени предусматривают виртуальное судопроизводство и соответствуют разделам 36(3) и (4) Конституции Нигерии. В связи с этим будет уместно заявить, что с учетом конституционных положений,

законодательных и судебных полномочий цифровые виртуальные судебные разбирательства являются законными, конституционными и допустимыми в нигерийской судебной системе.

4. Правовые и социально-экономические проблемы, связанные с цифровым виртуальным судопроизводством в Нигерии

Следует отметить, что введение виртуального судопроизводства в Нигерии является весьма позитивным событием, и многие отмечают его многочисленные преимущества. Однако эта практика сталкивается в Нигерии также с множеством юридических и социально-экономических проблем. Эти проблемы и сопутствующие им вопросы заслуживают рассмотрения с целью их устранения, чтобы обеспечить беспрепятственную практику виртуального судопроизводства в Нигерии.

4.1. Вопрос о конституционности виртуального судопроизводства в Нигерии

Одним из основных вопросов, возникших в связи с практикой виртуальных слушаний, является вопрос об их конституционности. Этот вопрос связан с тем, что в разделе 36 Конституции Нигерии не содержится прямого упоминания о цифровых виртуальных судебных заседаниях. Речь идет о том, что разделы 36(3) и (4) Конституции предусматривает, что слушания в судах и трибуналах должны проводиться публично. Именно при толковании этого подраздела возникло множество вопросов. Мнения практикующих юристов, ученых, преподавателей права, экспертов и, вероятно, даже судей по этому поводу разделились. Одни правоведы считают, что цифровые виртуальные судебные процессы нарушают конституционное требование о публичном слушании, поскольку представители общественности не смогут участвовать в виртуальном судебном заседании. Они также утверждают, что, учитывая требования Конституции, суды должны обеспечивать публичный доступ, за исключением тех очень ограниченных случаев, когда это необходимо для обеспечения общественной безопасности или охраны здоровья населения. По мнению этих ученых, цифровое виртуальное судопроизводство, как правило, ограничивает участие общественности в судебных процессах, поскольку не каждый может себе это позволить. В связи с этим они считают, что практические рекомендации и указания большинства судов, разрешающие и допускающие виртуальное цифровое судопроизводство, не соответствуют Конституции Нигерии. Однако достаточно сказать, что этот аргумент был опровергнут решением Верховного суда в деле Lagos State V Ekiti State Government (см. выше), где рассматривался вопрос о конституционности виртуального слушания. Генеральный прокурор штата Лагос и генеральный прокурор штата Экити обратились в Верховный суд с этой проблемой. Суд принял справедливое, хотя для многих и неожиданное решение о том, что виртуальное судопроизводство в Нигерии не противоречит Конституции и что оно осуществляется в соответствии с положениями Конституции Нигерии.

4.2. Проблемы доказательной базы

Проблема доказательной базы очень важна в любом судебном процессе. Доказательства – это ось, на которой держится судебный процесс. Дела проигрываются и выигрываются в зависимости от наличия или отсутствия доказательств. Как известно, для проверки представленных в суде доказательств часто вызываются

свидетели, которые должны пройти через перекрестный допрос. Хотя нельзя сказать, что в цифровом виртуальном судопроизводстве эта возможность полностью отсутствует, ее эффективность и действенность резко снижаются. Кроме того, цифровые виртуальные судебные процессы ставят перед судом проблему оценки достоверности показаний свидетеля. Качество видеозаписи и технологические сбои могут помешать суду воспринять показания свидетеля. Очевидна также необходимость приведения процесса представления доказательств и проверки их допустимости в соответствие практике традиционной судебной системы. Дело в том, что статьи 86 и 90 Закона о доказательствах предусматривают представление доказательств в их физической форме. Это означает, что доказательства в виде электронных копий или представленные с помощью цифровых платформ не признаются допустимыми. Кроме того, к рассмотрению может быть представлен и приобщен к делу подделанный документ, так как изменения или искажения в документе сложно выявить на экране. Отсутствие определенных рекомендаций и указаний относительно порядка представления доказательств в цифровом виртуальном судопроизводстве приводит к юридическим проблемам.

4.3. Исполнение постановлений

В отличие от привычных физических процедур исполнение судебных решений, таких как вручение документов или обеспечение исполнения решений, может стать более сложной задачей, когда речь идет о цифровом виртуальном судопроизводстве. Эта проблема усугубляется обилием проблем, которые возникают в среде цифровых технологий.

4.4. Цифровая грамотность и технофобия

Цифровое виртуальное судопроизводство во многом зависит от навыка использования цифровых технологий. Чтобы ориентироваться в этой практике, сторонам, и особенно юристам, необходима компьютерная и цифровая грамотность. Многие люди, не владеющие компьютерной грамотностью, уже поставлены в невыгодное положение. В их числе лица пожилого возраста, которые испытывают страх перед технологиями, вместо того чтобы осваивать и использовать их. Кроме того, в невыгодном положении оказываются пожилые судьи и практикующие юристы, которые привыкли к работе с бумагами и физическому присутствию в суде.

4.5. Проблемы инфраструктуры

Трудно переоценить важность создания инфраструктуры для беспрепятственного и эффективного проведения виртуальных судебных заседаний в цифровом формате. Для проведения виртуальных процессов необходимы стабильное и бесперебойное подключение к Интернету, электроснабжение и доступ к электронным устройствам. Это серьезная проблема, с которой сталкивается система эксплуатации цифровых технологий в Нигерии. В большинстве регионов страны нет постоянного электропитания. Качество работы Сети также является одной из основных проблем, так как соединения часто прерываются, и виртуальные судебные заседания ни в коей мере не защищены от этих проблем.

5. Представление и анализ данных

В следующем разделе представлены и проанализированы данные, полученные с помощью анкетирования в сети Интернет.

5.1. Размер выборки и методы изучения

Для достижения достаточно широкого охвата респондентов в Нигерии было проведено анкетирование в сети Интернет. Итоговая выборка исследования составила 303 респондента, проживающих в различных геополитических зонах Нигерии. Для отбора респондентов в исследовании использовался метод простой случайной выборки, который обладает следующими преимуществами:

– метод наиболее эффективен при отборе респондентов из неоднородных групп населения;

– результат, полученный при использовании данного метода, свободен от предвзятости и беспристрастен;

– использование метода случайной выборки для выявления респондентов не представляет сложностей и менее трудоемко;

– метод считается актуальным при использовании гибридного подхода к правовым исследованиям.

5.2. Анализ данных

Данные, полученные или сгенерированные на основе проведенного анкетирования, представлены ниже (табл. 1–6).

Таблица 1 отражает количество и соотношение респондентов, проживающих в различных регионах страны.

Таблица 1. Соотношение ответов на вопрос о месте жительства (303 ответа)

№	Геополитические зоны	Кол-во	%
1	Северо-центральная	35	11,6
2	Северо-восточная	37	12,2
3	Северо-западная	29	9,6
4	Юго-восточная	67	22,1
5	Южная	79	26,1
6	Юго-западная	56	18,5
	Всего	303	100

Таблица 2 показывает количество и соотношение ответов о перспективности внедрения виртуальных судебных заседаний при исполнении правосудия в Нигерии.

Таблица 2. Соотношение ответов респондентов на вопрос «Считаете ли вы, что внедрение виртуальных судебных заседаний в Нигерии перспективно?» (303 ответа)

Ответ	Кол-во	%
Да	260	85,8
Нет	43	14,2
Всего	303	100

В табл. 3 показано количество и соотношение ответов респондентов на вопрос о преимуществах виртуальных судебных заседаний в Нигерии.

Таблица 3. Соотношение ответов респондентов на вопрос о преимуществах виртуальных судебных заседаний (263 ответа, можно выбрать более 1 ответа)

Преимущества виртуальных судебных заседаний	Кол-во	%
Удобство для всех сторон процесса	157	59,7
Избавляет от ненужных потерь времени на поездки для физического участия в судебных заседаниях	214	81,4
Подчеркивает принципы справедливого разбирательства, предусмотренные Конституцией Нигерии	194	73,8
Низкие затраты и экономическая выгода	106	40,3
Избавляет от проблемы больших расстояний, которая может служить барьером для отправления правосудия	210	79,8
Позволяет вести точный учет и сохранять информацию о судебных заседаниях	131	49,8
Снижает нагрузку на судью и адвокатов при ведении протокола	185	70,3

Таблица 4 отражает количество и соотношение ответов респондентов на вопрос о существовании сложностей с внедрением виртуальных судебных заседаний в Нигерии.

Таблица 4. Соотношение ответов респондентов на вопрос о существовании сложностей с внедрением виртуальных судебных заседаний в Нигерии (303 ответа)

Ответ	Кол-во	%
Да	259	85,5
Нет	44	14,5
Всего	303	100

В табл. 5 представлено количество и соотношение ответов респондентов на вопрос о проблемах, которые могут затруднить внедрение виртуальных судебных заседаний в Нигерии.

Таблица 5. Соотношение ответов респондентов на вопрос о сложностях с внедрением виртуальных судебных заседаний в Нигерии (263 ответа, можно выбрать более 1 ответа)

Сложности виртуальных судебных заседаний	Кол-во	%
Недостаточное правовое регулирование виртуальных судебных заседаний	210	79,8
Сложность проведения виртуальных судебных заседаний может приводить к потере информации	201	76,4
Злоумышленники могут взломать цифровую платформу	149	56,7
Коррупция среди сотрудников судебной системы может приводить к манипулированию процессом	200	76
Неэффективность сетевого соединения	152	57,8
Ненадежность электроснабжения	141	53,6
Цифровая неграмотность и неумение пользоваться программным обеспечением большинства юристов и тяжущихся	191	72,6

В табл. 6 можно видеть ответы респондентов на вопрос о возможных решениях проблемы виртуальных судебных заседаний в Нигерии.

Таблица 6. Соотношение ответов респондентов на вопрос о возможных решениях проблемы виртуальных судебных заседаний в Нигерии (263 ответа, можно выбрать более 1 ответа)

Стратегия, способствующая внедрению виртуальных судебных заседаний	Кол-во	%
Пересмотр законов и судебных правил для адекватного регулирования виртуальных судебных заседаний	213	81
Обеспечение дополнительных мер по безопасному ведению протоколов и хранению информации	216	82,1
Строгие меры пресечения для лиц, причастных к цифровым преступлениям	141	53,6
Обучение юристов использованию виртуальных судебных заседаний	190	72,2
Обеспечение эффективной и стабильной работы сети со стороны провайдеров	161	61,2
Обеспечение надежного электроснабжения	129	49

5.3. Обсуждение полученных результатов

Данные, полученные в ходе исследования с помощью анкетирования, представлены в табличном виде и проанализированы следующим образом. Выборку исследования составили 303 респондента, ответившие на вопросы анкеты. Все они являются нигерийцами, проживают в различных частях страны (табл. 1), обладают соответствующими знаниями и хорошо информированы о перспективах и проблемах цифрового виртуального судопроизводства в Нигерии. Из табл. 2 видно, что 85,5 % респондентов подтверждают, что внедрение цифрового виртуального судопроизводства имеет ряд перспектив для совершенствования отправления правосудия в Нигерии. В связи с этим респонденты отметили следующие преимущества цифрового виртуального судопроизводства (табл. 3):

1. 59,7 и 81,4 % респондентов отметили, что это удобно и избавляет от лишних потерь времени на дорогу для физического присутствия на судебных заседаниях.

2. 73,8 % респондентов согласились с тем, что этот подход подчеркивает принципы справедливого судебного разбирательства, предусмотренные Конституцией Нигерии.

3. 40,3 и 79,8 % также отметили, что виртуальное судопроизводство дешевле и экономически эффективнее и избавляет от проблемы больших расстояний, которая может служить препятствием для отправления правосудия.

4. 49,8 % отметили, что виртуальное судопроизводство облегчает точный учет и надежное хранение материалов судебных заседаний.

5. Кроме того, 70,3 % респондентов высказали мнение, что оно снижает нагрузку на судью и адвокатов при ведении протокола.

Однако, несмотря на привлекательные и убедительные перспективы, которые открывают цифровые технологии, 85,8 % респондентов подтверждают (табл. 4), что в Нигерии существуют проблемы с внедрением и использованием цифрового виртуального судопроизводства. В связи с этим выделяют следующие проблемы (табл. 5): 79,8 % респондентов заявили о недостаточном правовом регулировании использования цифрового виртуального судопроизводства. 76,4 % участников считают, что сложная природа цифрового виртуального судопроизводства может привести

к необратимой потере информации. Полученные результаты свидетельствуют о том, что сложная природа цифровых технологий и некачественные методы работы могут привести к потере информации и дать возможность интернет-мошенникам влиять на использование цифровых платформ. 56,7 % интервьюируемых отметили, что интернет-мошенники могут взломать цифровую платформу. 76 % заявили, что существуют также проблемы, связанные с коррупцией со стороны сотрудников судебной системы, которые могут манипулировать процессами. 57,8 и 53,6 % респондентов согласились с тем, что серьезной проблемой могут стать плохая сеть и ненадежное электроснабжение. Полученные результаты также свидетельствуют о том, что Нигерия все еще является развивающейся страной, которая пока не смогла решить проблемы плохого интернет-соединения и электроснабжения, что затрудняет развитие цифровых технологий в стране. Кроме того, 72,6 % респондентов отметили, что существует также проблема неграмотности и неумения работать с цифровым виртуальным программным обеспечением со стороны большинства адвокатов и участников судебных процессов.

Несмотря на перечисленные проблемы цифрового виртуального судопроизводства в Нигерии, можно констатировать, что его преимущества и перспективы многочисленны. Кроме того, с развитием глобальной цифровой среды нигерийцы не могут позволить себе отстать от общемировых тенденций. В табл. 6 показаны возможные решения для устранения вышеуказанных правовых и социально-экономических проблем, связанных с внедрением цифрового виртуального судопроизводства в Нигерии:

1. 81 % респондентов считают, что для адекватного обеспечения цифрового виртуального судопроизводства необходимо пересмотреть и законы, и правила судебных заседаний.

2. 82,1 % участников отметили, что необходимо обеспечить дополнительное резервное копирование при хранении информации и ведении протоколов судебных заседаний.

3. 53,6 % интервьюируемых назвали строгое преследование лиц, причастных к цифровым преступлениям, в качестве меры по расширению использования цифрового виртуального судопроизводства в Нигерии.

4. Кроме того, 72,2 % респондентов высказали мнение о необходимости проведения разъяснительной работы и обучения юристов-практиков по вопросам использования цифровых виртуальных судебных процедур.

5. Наконец, 61,2 % участников заявили о необходимости повышения эффективности и качества связи со стороны интернет-провайдеров, а 49 % респондентов – о необходимости стабильного электроснабжения.

Заключение

Исследование позволило изучить возможности и перспективы цифрового виртуального судопроизводства в Нигерии. В ходе исследования было также выявлено, что Конституция Нигерии не предусматривает и не регулирует в явном виде цифровые виртуальные судебные процедуры, однако при тщательном изучении разделов 36(3) и (4) Конституции Нигерии можно сделать вывод о том, что цифровые виртуальные судебные процедуры подразумеваются и признаются законными. Кроме того, в исследовании отмечается, что данная позиция закона была подтверждена в судебном

порядке Верховным судом Нигерии. Поскольку Конституция страны предусматривает полномочия глав различных судов Нигерии устанавливать правила, касающиеся деятельности их судов, главы Верховного суда штата Лагос и Национального промышленного суда ввели в действие свои практические указания и включили в них регулирование цифрового виртуального судопроизводства.

Следует, однако, отметить, что, хотя цифровое виртуальное судопроизводство открывает большие возможности для повышения эффективности и доступности судебной системы Нигерии, существует ряд правовых и социально-экономических проблем, которые могут повлиять на его жизнеспособность. Такие проблемы были выявлены в данном исследовании, в связи с чем было выработано несколько важных соображений и рекомендаций:

1. В соответствии с правом на неприкосновенность частной жизни, гарантированным главой 4 Конституции Федеративной Республики Нигерия от 1999 г., суды должны принять самые строгие меры безопасности для защиты конфиденциальной информации, предотвращения несанкционированного доступа и сохранения конфиденциальности судебного разбирательства.

2. Суды должны усовершенствовать существующие руководства и методические рекомендации, включив в них указания и стандарты по устранению технических неполадок и ведению виртуального судопроизводства, уделяя особое внимание правилам представления и рассмотрения доказательств.

3. Правительство и заинтересованные лица должны взять на себя обязательство инвестировать средства в создание надежной и стабильной интернет-связи, а также электроснабжения в масштабах всей страны, чтобы обеспечить бесперебойное проведение виртуальных заседаний.

4. Правительство и судебные органы Нигерии должны регулярно организовывать программы обучения для адвокатов, судей и вспомогательного персонала судов с целью повышения их цифровой грамотности, что позволит им эффективно использовать платформы и инструменты виртуального судопроизводства.

5. Судам, проводящим виртуальные слушания, следует улучшить работу по обеспечению доступности своих процедур для всех сторон, включая стороны с ограниченными ресурсами, путем размещения ссылок в специально предназначенном для этого месте с открытым доступом, а также путем предоставления необходимых технологий и поддержки для преодоления цифрового неравенства.

6. Судам следует предпринять целенаправленные усилия по внедрению процедуры удаленного принесения присяги для обеспечения достоверности свидетельских показаний, как это принято в традиционном суде.

Список литературы

Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior*, *2*(1), 1–6. https://doi.org/10.1037/tmb0000030

Bandes, S. A., & Feigenson, N. (2020). Virtual trials: Necessity, invention, and the evolution of the courtroom. *Buffalo Law Review*, *68*(5), 1275–1352. https://doi.org/10.2139/ssrn.3683408

Bandes S. A., & Feigenson, N. (2021). Empathy and remote legal proceedings. *Southwestern Law Review*, *51*(1), 20–39. https://clck.ru/36dpJt

Bannon, A., & Keith, D. (2021). Remote Court: Principles for Virtual Proceedings during the Covid-19 Pandemic and Beyond. *Northwestern University Law Review*, *115*(6), 1875–1897. https://clck.ru/36ct2V

Bild, E., Redman, A., Newman, E. J., Muir, B. R., Tait, D., & Schwarz, N. (2021). Sound and credibility in the virtual court: Low audio quality leads to less favorable evaluations of witnesses and lower weighting of evidence. *Law and Human Behavior*, *45*(5), 481–495. https://doi.org/10.1037/lhb0000466

Bunjavec, T. (2020). *Judicial Self-Governance in the new Millennium – an Institutional and Policy Framework*. Springer. https://doi.org/10.1007/978-981-33-6506-3

Derksen, D. G., Giroux, M. E., Connolly, D. A., Newman, E. J., & Bernstein, D. M. (2020). Truthiness and law: Nonprobative photos bias perceived credibility in forensic contexts. *Applied Cognitive Psychology*, *34*(6), 1335–1344. https://doi.org/10.1002/acp.3709

Elek, J. K., Ware, L. J., & Ratcliff, J. J. (2012). Knowing when the camera lies: Judicial instructions mitigate the camera perspective bias. *Legal and Criminological Psychology*, *17*(1), 123–135. https://doi.org/10.1111/j.2044-8333.2010.02000.x

Fauville, G., Luo, M., Queiroz, A. C. M., Bailenson, J. N., & Hancock, J. (2021). Nonverbal mechanisms predict Zoom fatigue and explain why women experience higher levels than men. *SSRN Electronic Journal*, 1–18. https://doi.org/10.2139/ssrn.3820035

Feigenson, N. (2010). Visual evidence. *Psychonomic Bulletin & Review*, *17*(2), 149–154. https://doi.org/10.3758/PBR.17.2.149

Goethe, O., Sørum, H., & Johansen, J. (2021). The effect or non-effect of virtual versus non-virtual backgrounds in digital learning. In T. Ahram, & R. Taiar (Eds.), *Lecture notes in networks and systems: Vol. 319. Human interaction, emerging technologies and future systems* (pp. 274–281). Springer. https://doi.org/10.1007/978-3-030-85540-6_35

Granot, Y., Feigenson, N., Balcetis, E., & Tyler, T. (2018). In the eyes of the law: Perception versus reality in appraisals of video evidence. *Psychology, Public Policy, and Law*, *24*(1), 93–104. https://doi.org/10.1037/law0000137

Hans, V. P. (2022). Virtual juries. *DePaul Law Review*, *71*(2), 301–330. http://dx.doi.org/10.2139/ssrn.3860165

Hwang, A. H.-C., Wang, C. Y., Yang, Y.-Y., & Won, A. S. (2021). Hide and seek: Choices of virtual backgrounds in video chats and their effects on perception. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 5, Iss. CSCW2, pp. 1–22). New York, NY. https://doi.org/10.1145/3476044

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *University of New South Wales Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Machado, M., Sousa, M., Rocha, V. & Isidro, A. (2018). Innovation in judicial services: a study of innovation models in labor courts. *Innovation & Management Review*, *15*(2), 155–173. https://doi.org/10.1108/INMR-04-2018-010

Meredith, R., David, T., & McCurdy, M. (2021). Justice reimagined: challenges and opportunities with implementing virtual courts. *Current Issues in Criminal Justice*, *33*(4), 1–17. https://doi.org/10.1080/10345329.2020.1859968

Mohamad, A. M., & Sule, I. (2021). ICT-Enabled Applications for Decision-Making by the Courts: Experiences from Malaysia and Nigeria. *International Journal of Law, Government and Communication*, *6*(22), 189–196. https://doi.org/10.35631//ijlgc.6220018

Nir, E., & Musial, J. (2022). Zooming in: Courtrooms and defendants' rights during the COVID-19 pandemic. *Social & Legal Studies*, *31*(5), 725–745. https://doi.org/10.1177/09646639221076099

Olubukola, O., & Abimbola, D. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 21–38. https://doi.org/10.36745/ijca.448

Rossner, M. (2021). Remote rituals in virtual courts. *Journal of Law and Society*, *48*(3), 334–361. https://doi.org/10.1111/jols.12304

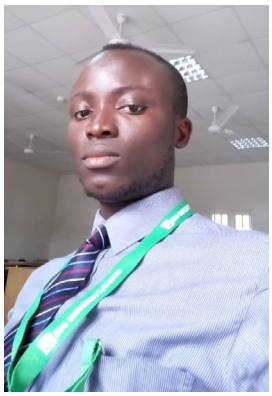
Sanson, M., Crozier, W. E., & Strange, D. (2020). Court case context and fluency-promoting photos inflate the credibility of forensic science. *Zeitschrift für Psychologie*, *228*(3), 221–225. https://doi.org/10.1027/2151-2604/a000415

Tait, D., & Tay, V. (2019). *Virtual court study: Report of a pilot test 2018*. Western Sydney University. https://doi.org/10.26183/5d01d1418d757

Thornburg, E. G. (2021). Observing online courts: Lessons from the pandemic. *SSRN Electronic Journal*, *54*(3), 181–244. https://doi.org/10.2139/ssrn.3696594

Winter, B., Daguna, J., & Matlock, T. (2018). Metaphor-enriched social cognition and spatial bias in the courtroom. *Metaphor and the Social World*, *8*(1), 81–99. https://doi.org/10.1075/msw.17001.win

Информация об авторах



Айдоноджи Пол Атагамен – PhD, преподаватель права, координатор отдела аспирантуры, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: aidonojie.paul@edouniversity.edu.ng
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Вакили Самину Абача – ассистент исследователя, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: wakili18.saminu@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0000-7043-286X

Аюба Давид – ассистент исследователя, факультет права, Государственный университет Эдо-Узайруэ
Адрес: 689M+PP5, 312107, Нигерия, штат Эдо, г. Иямхо, Аучи/Абуджа Экспресс Вей
E-mail: ayuba18.david@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0008-7706-9627

Вклад авторов

Пол А. Айдоноджи осуществлял общее руководство и постановку задач исследования; поиск и подбор научной литературы; критическую оценку интерпретации результатов исследования; формулировку ключевых выводов, предложений и рекомендаций; утверждение окончательного варианта статьи.
Самину А. Вакили осуществлял анализ национального законодательства; выполнял интерпретацию результатов исследования; организовал проведение социологического опроса и подготовку чернового рукописи.
Давид Аюба занимался сбором и анализом литературы и законодательства; проводил социологический опрос; выполнял интерпретацию результатов исследования; осуществлял подготовку чистовика рукописи.

Конфликт интересов

Авторы сообщают 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: 10.91 / Государство и право отдельных стран
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 18 августа 2023 г.
Дата одобрения после рецензирования – 25 октября 2023 г.
Дата принятия к опубликованию – 30 ноября 2023 г.
Дата онлайн-размещения – 15 декабря 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.48

Effectiveness of the Administration of Justice in Nigeria Under the Development of Digital Technologies

Paul A. Aidonojie ✉

Edo State University Uzairue
Iyamho, Nigeria

Saminu A. Wakili

Edo State University Uzairue
Iyamho, Nigeria

David Ayuba

Edo State University Uzairue
Iyamho, Nigeria

Keywords

administration of justice,
court,
digital platform,
digital technologies,
electronic justice,
electronic record keeping,
law,
online court proceedings,
online dispute management,
virtualization of court proceedings

Abstract

Objective: the traditional Nigerian judicial system has long been associated with a conservative approach and traditional methodologies of justice administration. As a developing country, Nigeria has benefited immensely from the advancement of digital technology, especially in the legal field. This is due to the fact that modern digital technologies are being rapidly adopted in Nigeria's judicial processes for effective justice administration. However, despite the promise of digital technology, there are legal and socio-economic challenges in Nigeria that may affect its successful utilization in legal proceedings. This justifies the focus of the study – to identify the legal and socio-economic challenges of digitalization of court proceedings in Nigeria.

Methods: the study combines doctrinal and non-doctrinal approaches. The former ensures theoretical understanding of the conceptual issues

✉ Corresponding author

and prospects of court proceedings virtualization. It also allows exploring, based on primary and secondary sources (laws, monographs, research articles and internet resources), the legal and socio-economic challenges of the use of digital technologies in court proceedings. The non-doctrinal approach consists in polling, describing and analyzing the results of a sociological survey. The survey was conducted among Nigeria residents to reveal their attitudes towards innovations in digitalization and virtualization of court proceedings as well as the challenges posed by these processes.

Results: the study revealed that the use of digital technologies in court proceedings in Nigeria has several prospects of ensuring effective justice administration and accurate recording and storage of information. Along with the benefits, challenges are shown that may reduce the effectiveness of court proceedings digitalization.

Scientific novelty: consists in investigating the use of digital technology in Nigerian court proceedings and identifying the prospects of improving the efficiency of justice administration in Nigeria under digitalization, as well as the challenges arising from this trend.

Practical significance: the study will enable stakeholders in the Nigerian legal sector to identify legal and socio-economic challenges that may adversely affect and render ineffective the use of digital technologies in legal proceedings. In addition, the article offers practical recommendations to address these challenges.

For citation

Aidonojie, P. A., Wakili, S. A., & Ayuba, D. (2023). Effectiveness of the administration of justice in Nigeria under the development of digital technologies. *Journal of Digital Technologies and Law, 1*(4), 1105–1131. https://doi.org/10.21202/jdtl.2023.48

References

Bailenson, J. N. (2021). Nonverbal overload: A theoretical argument for the causes of Zoom fatigue. *Technology, Mind, and Behavior*, *2*(1), 1–6. https://doi.org/10.1037/tmb0000030

Bandes, S. A., & Feigenson, N. (2020). Virtual trials: Necessity, invention, and the evolution of the courtroom. *Buffalo Law Review*, *68*(5), 1275–1352. https://doi.org/10.2139/ssrn.3683408

Bandes S. A., & Feigenson, N. (2021). Empathy and remote legal proceedings. *Southwestern Law Review*, *51*(1), 20–39. https://clck.ru/36dpJt

Bannon, A., & Keith, D. (2021). Remote Court: Principles for Virtual Proceedings during the Covid-19 Pandemic and Beyond. *Northwestern University Law Review*, *115*(6), 1875–1897. https://clck.ru/36ct2V

Bild, E., Redman, A., Newman, E. J., Muir, B. R., Tait, D., & Schwarz, N. (2021). Sound and credibility in the virtual court: Low audio quality leads to less favorable evaluations of witnesses and lower weighting of evidence. *Law and Human Behavior*, *45*(5), 481–495. https://doi.org/10.1037/lhb0000466

Bunjavec, T. (2020). *Judicial Self-Governance in the new Millennium – an Institutional and Policy Framework*. Springer. https://doi.org/10.1007/978-981-33-6506-3

Derksen, D. G., Giroux, M. E., Connolly, D. A., Newman, E. J., & Bernstein, D. M. (2020). Truthiness and law: Nonprobative photos bias perceived credibility in forensic contexts. *Applied Cognitive Psychology*, *34*(6), 1335–1344. https://doi.org/10.1002/acp.3709

Elek, J. K., Ware, L. J., & Ratcliff, J. J. (2012). Knowing when the camera lies: Judicial instructions mitigate the camera perspective bias. *Legal and Criminological Psychology*, *17*(1), 123–135. https://doi.org/10.1111/j.2044-8333.2010.02000.x

Fauville, G., Luo, M., Queiroz, A. C. M., Bailenson, J. N., & Hancock, J. (2021). Nonverbal mechanisms predict Zoom fatigue and explain why women experience higher levels than men. *SSRN Electronic Journal*, 1–18. https://doi.org/10.2139/ssrn.3820035

Feigenson, N. (2010). Visual evidence. *Psychonomic Bulletin & Review*, *17*(2), 149–154. https://doi.org/10.3758/PBR.17.2.149

Goethe, O., Sørum, H., & Johansen, J. (2021). The effect or non-effect of virtual versus non-virtual backgrounds in digital learning. In T. Ahram, & R. Taiar (Eds.), *Lecture notes in networks and systems: Vol. 319. Human interaction, emerging technologies and future systems* (pp. 274–281). Springer. https://doi.org/10.1007/978-3-030-85540-6_35

Granot, Y., Feigenson, N., Balcetis, E., & Tyler, T. (2018). In the eyes of the law: Perception versus reality in appraisals of video evidence. *Psychology, Public Policy, and Law*, *24*(1), 93–104. https://doi.org/10.1037/law0000137

Hans, V. P. (2022). Virtual juries. *DePaul Law Review*, *71*(2), 301–330. http://dx.doi.org/10.2139/ssrn.3860165

Hwang, A. H.-C., Wang, C. Y., Yang, Y.-Y., & Won, A. S. (2021). Hide and seek: Choices of virtual backgrounds in video chats and their effects on perception. In *Proceedings of the ACM on Human-Computer Interaction* (Vol. 5, Iss. CSCW2, pp. 1–22). New York, NY. https://doi.org/10.1145/3476044

Legg, M., & Song, A. (2021). The courts, the remote hearing and the pandemic: From action to reflection. *University of New South Wales Law Journal*, *44*(1), 126–166. https://doi.org/10.53637/ZATE4122

Machado, M., Sousa, M., Rocha, V. & Isidro, A. (2018). Innovation in judicial services: a study of innovation models in labor courts. *Innovation & Management Review*, *15*(2), 155–173. https://doi.org/10.1108/INMR-04-2018-010

Meredith, R., David, T., & McCurdy, M. (2021). Justice reimagined: challenges and opportunities with implementing virtual courts. *Current Issues in Criminal Justice*, *33*(4), 1–17. https://doi.org/10.1080/10345329.2020.1859968

Mohamad, A. M., & Sule, I. (2021). ICT-Enabled Applications for Decision-Making by the Courts: Experiences from Malaysia and Nigeria. *International Journal of Law, Government and Communication*, *6*(22), 189–196. https://doi.org/10.35631//ijlgc.6220018

Nir, E., & Musial, J. (2022). Zooming in: Courtrooms and defendants' rights during the COVID-19 pandemic. *Social & Legal Studies*, *31*(5), 725–745. https://doi.org/10.1177/09646639221076099

Olubukola, O., & Abimbola, D. (2022). Remote Court Proceedings in Nigeria: Justice Online or Justice on the Line. *International Journal for Court Administration*, *13*(2), 21–38. https://doi.org/10.36745/ijca.448

Rossner, M. (2021). Remote rituals in virtual courts. *Journal of Law and Society*, *48*(3), 334–361. https://doi.org/10.1111/jols.12304

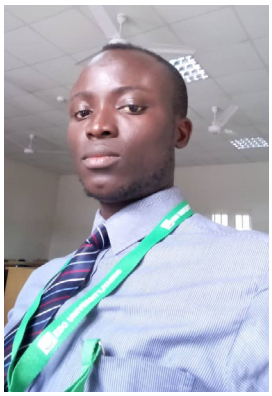
Sanson, M., Crozier, W. E., & Strange, D. (2020). Court case context and fluency-promoting photos inflate the credibility of forensic science. *Zeitschrift für Psychologie*, *228*(3), 221–225. https://doi.org/10.1027/2151-2604/a000415

Tait, D., & Tay, V. (2019). *Virtual court study: Report of a pilot test 2018*. Western Sydney University. https://doi.org/10.26183/5d01d1418d757

Thornburg, E. G. (2021). Observing online courts: Lessons from the pandemic. *SSRN Electronic Journal*, *54*(3), 181–244. https://doi.org/10.2139/ssrn.3696594

Winter, B., Daguna, J., & Matlock, T. (2018). Metaphor-enriched social cognition and spatial bias in the courtroom. *Metaphor and the Social World*, *8*(1), 81–99. https://doi.org/10.1075/msw.17001.win

Authors information



Paul Atagamen Aidonojie – PhD, Lecturer, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: aidonojie.paul@edouniversity.edu.ng
ORCID ID: https://orcid.org/0000-0001-6144-2580
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57221636261
Google Scholar ID: https://scholar.google.com/citations?user=0h9E2ZIAAAAJ

Saminu Abacha Wakili – Assistant Researcher, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: wakili18.saminu@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0000-7043-286X

David Ayuba – Assistant Researcher, Faculty of Law, Edo State University Uzairue
Address: 689M+PP5, 312107, Auchi/Abuja Express Way, Iyamho, Edo State, Nigeria
E-mail: ayuba18.david@edouniversity.edu.ng
ORCID ID: https://orcid.org/0009-0008-7706-9627

Authors' contributions

Paul Atagamen Aidonojie provided overall guidance and set the study objectives; searched and selected the scientific literature; critically evaluated the interpretation of the study results; formulated the key findings, suggestions and recommendations; and approved the final version of the article.
Saminu Abacha Wakili analyzed the national legislation; interpreted the study findings; organized the sociological survey; and drafted the manuscript.
David Ayuba collected and analyzed literature and legislation; conducted the sociological survey; interpreted the study results; and prepared the manuscript.

Conflict of interest

The authors declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – August 18, 2023
Date of approval – October 25, 2023
Date of acceptance – November 30, 2023
Date of online placement – December 15, 2023