ISSN 2949-2483

Volume 3 Number 3

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2025

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Том 3, № 3
2025
DOI: 10.21202/2949-2483.2025.3

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, Республика Татарстан, 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 – 25 сентября 2025 г. Дата онлайн-размещения на сайте https://www.lawjournal.digital – 30 сентября 2025 г.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 3, № 3
2025
DOI: 10.21202/2949-2483.2025.3
ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
eISSN 2949-2483

Содержание

Научная статья
УДК 34:004:341.4:004.8
EDN: https://elibrary.ru/gcvuaw
DOI: https://doi.org/10.21202/jdtl.2025.15

Международные основы правового регулирования индустрии центров обработки данных в арктических государствах и Антарктике

Наталья Игоревна Шумакова

Южно-Уральский государственный университет (национальный исследовательский университет), Челябинск, Россия

Ключевые слова

Антарктика,
Арктика,
коренные народы,
международное право,
право коренных народов,
право,
центры обработки данных,
цифровые технологии,
экологическая безопасность,
экологическое право

Аннотация

Цель: критически оценить эффективность существующих международных правовых норм в условиях новых вызовов технологического прогресса, связанных с развитием индустрии центров обработки данных в арктических государствах и Антарктике.

Методы: методологическую основу исследования составляет комплекс специальных и общих методов научного познания, включая юридическую компаративистику, контент-анализ, дедукцию, индукцию, формально-логический метод и анализ документов. Автор уделяет внимание междисциплинарным подходам для объективной оценки экологических, социальных и правовых рисков, возникающих вследствие роста индустрии центров обработки данных в регионах с повышенной климатической и социальной уязвимостью.

Результаты: проведен анализ международных правовых актов, регулирующих деятельность центров обработки данных в полярных регионах. Выявлены ключевые риски, делящиеся на экологические (нестабильность локальных экосистем, неадаптивность к быстрым изменениям, риск потери биологического разнообразия и выбросы парниковых газов) и социальные (маргинализация и нарушение прав коренных народов, утрата традиционных культур и образа жизни, рост социальной напряженности). Указана неизбежность появления новых конфликтов и вызовов вследствие недостаточной эффективности национальных и международных механизмов регулирования. Констатирована необходимость создания специализированных международных правовых инструментов, учитывающих специфику экологической безопасности полярных территорий.

Научная новизна: статья впервые дает комплексную картину совокупных рисков и недостатков действующего международного регулирования индустрии центров обработки данных в арктических государствах и Антарктике. Проведен детальный сравнительный анализ нормативной базы, показана несоответственность применения принципов «мягкого права» в полярных регионах в эпоху четвертой технологической революции. Обосновано требование о создании новых сертификационных и отчетных процедур на всем жизненном цикле центров обработки данных с учетом правового и культурного контекста.

Практическая значимость: результаты работы ориентированы на совершенствование международной и национальной политики в сфере регулирования индустрии центров обработки данных, разработку стандартов сертификации и отчетности, эффективных в условиях климатических, социальных и экономических особенностей арктических стран и Антарктики. Направлены на минимизацию негативного влияния антропогенных факторов и обеспечение баланса между индустриальным развитием и сохранением уникальных природных и культурных ландшафтов.

Для цитирования

Шумакова, Н. И. (2025). Международные основы правового регулирования индустрии центров обработки данных в арктических государствах и Антарктике. *Journal of Digital Technologies and Law*, *3*(3), 369–396. https://doi.org/10.21202/jdtl.2025.15

Содержание

Введение

Стремительный темп продолжающейся четвертой технологической революции сопровождается ростом развития новых индустрий, одной из которых является строительство центров обработки данных (далее – ЦОД). Энергоемкие и требующие поддержания определенного уровня температуры ЦОД протянулись до крайних точек земного шара – Арктики и Антарктики. Арктические государства привлекательны для расположения ЦОД ввиду относительно низкой стоимости электроэнергии

и климатических условий, способствующих снижению затрат на охлаждение, в то время как в Антарктике рост антропогенной активности обусловлен необходимостью научных исследований ее регионов и популяризацией полярного туризма, которые также нуждаются в создании новых ЦОД и прокладке глубоководных морских кабелей для оперативной связи и своевременной передачи данных.

Уязвимость арктических и антарктических регионов перед антропогенными выбросами – общеизвестный факт, и защите их окружающей среды посвящен целый массив международных правовых актов. Тем не менее есть основания полагать, что в XXI в. не все государства, присоединившиеся к входящим в него конвенциям и декларациям, в достаточной степени соблюдают свои обязательства. В частности, это связано с реализацией целей Закона Евросоюза (далее – ЕС) «О критически важном сырье», таких как независимость входящих в него государств от третьих стран в вопросах обеспечения полезными ископаемыми[1] и др. Дополнительным фактором, указывающим на снижение эффективности действия международного права в вопросах изменения землепользования в арктических странах, является нарушение в них прав коренного населения под эгидой критической необходимости добычи ископаемых, требуемых для развития цифровых технологий и перехода на зеленую энергетику, – расплывчатые формулировки и критерии текущих правовых нормативных актов позволяют имплементировать политические решения, идущие против воли коренного населения, даже в тех странах, где представителям коренных народов предоставлена относительная автономия, признанная на конституционном уровне (Živojinović et al., 2024).

Вышеизложенным определена цель настоящей статьи – дать критическую оценку эффективности существующих международных норм права перед новыми вызовами технологического прогресса. Данная цель достигается посредством выявления специфических для арктических стран и Антарктики групп рисков, анализа общих и специальных международных правовых актов, определения роли данных территорий в обеспечении развития и функционирования ЦОД, а также идентификации рисков, связанных непосредственно с ростом индустрии ЦОД в их регионах. Основным назначением проведенного исследования является призыв к развитию специальных международных мер, способных нивелировать негативное воздействие новых видов антропогенной активности на территориях, от которых зависит климатическое благополучие всего человечества. Статья призывает к разработке единых требований к сертификации и отчетности всего периода жизни ЦОД, включая сопутствующие их созданию индустрии, а также мер ответственности за нарушения с учетом специфики экологической безопасности этих территорий, их культурных и социальных особенностей.

1. Арктика и Антарктика как зоны особых рисков, подлежащих международному регулированию

В условиях глобальных климатических изменений Арктика и Антарктика относятся к зонам особых экономических рисков. Повышение температуры приводит к тому, что полярные регионы стремительно нагреваются, тем самым провоцируя

[1] Regulation (EU) 2024/1252 of the European Parliament and of the Council of 11 April 2024. https://clck.ru/3NNWKX

истончение ледяных покровов, таяние морского льда и вечной мерзлоты, вызывая негативные изменения далеко за их пределами (Raimondi et al., 2024). Среди последствий исследователи называют нарушение климатических и геохимических циклов, которые не только ведут к потере биологического разнообразия и утере среды обитания для животных, но также и к социально-экономической деградации жителей арктических регионов, более того, на сегодняшний день речь уже идет о возможном достижении точки невозврата, после пересечения которой человечество столкнется с «каскадом неблагоприятных последствий» для всей планеты[2]. Согласно проведенным исследованиям в рамках проекта Horizon 2020 под управлением Университета Бергена, острее всего эффект глобального потепления, вызванного деятельностью человека, ощущается в Арктике – в Северном Ледовитом океане закисление из-за парниковых выбросов прогрессирует в 10 раз, а потепление – в два раза быстрее, чем где-либо в мире, что говорит о пересечении многих из точек невозврата как о состоявшемся факте[3]. Так, вместе с возрастанием содержания диоксида углерода (CO_2) в атмосфере и повышением температуры увеличиваются сезонные колебания парциального давления углекислого газа (pCO_2) и меняется водородный показатель (pH) воды, вследствие чего увеличивается летнее закисление океана, способное снизить устойчивость эндемических морских организмов к повышению летних температур (крылоногие моллюски, веслоногие рачки, полярная треска и т. д.), являющихся основным связующим звеном между зоопланктоном и морскими млекопитающими, морскими птицами и другими рыбами (Orr et al., 2022). Увеличение выбросов CO_2 является первопричиной поглощения водной поверхностью антропогенного углекислого газа (C_{ant}), что и есть главный фактор окисления открытого океана (Terhaar et al., 2020), притом от содержания кислорода (O_2) зависит сохранность морских экосистем, чувствительных к взаимосвязанным процессам потепления, закисления, деоксигинации[4] (снижения уровня кислорода), сокращения питательных веществ и первичной продукции[5]. Кроме того, ученые обращают внимание на так называемое арктическое усиление – доказанный факт того, что Арктика нагревается быстрее остального земного шара, новейшие исследования демонстрируют, что с 1979 по 2021 г. этот процесс протекал почти в четыре раза быстрее, чем где-либо, и это является индикатором того, что более ранние прогнозы скорости глобального потепления (в два раза быстрее, чем в других регионах) не могут считаться точными, поскольку в недостаточной степени оценивают развитие ситуации за последние 43 года – с начала спутниковых наблюдений отдельные районы в евразийском секторе Северного Ледовитого океана нагревались до семи раз быстрее земного шара, а в целом рост температуры в Арктике за данный период превышал скорость потепления на других территориях почти в четыре раза (Rantanen et al., 2022). Факторами изменения климата в Арктике также служат глобализация и цифровизация, поскольку на ее территории находятся залежи необходимых для «зеленого сдвига» – перехода на возобновляемые источники энергии в рамках стремления

2 EU. Understanding impacts of climate change on Earth's vulnerable polar regions. https://clck.ru/3NNWzc

3 EU. (2020). Our common future ocean in the Earth system. https://clck.ru/3NNX3x

4 FAQ: Ocean Deoxygenation. Scripps Institution of Oceanography. https://clck.ru/3NNX5m

5 Там же.

Европейского союза к нулевому выбросу углекислого газа к 2050 г. – полезных ископаемых, добыча которых продолжает расти (для обеспечения производств солнечных панелей, ветряных турбин, автомобильных аккумуляторов и т. д.), что не только влечет за собой необратимые воздействия на окружающую среду и изменения ландшафта, но и вызывает беспокойство (а иногда и социальную напряженность) среди местного населения (Živojinović et al., 2024). Среди положительных сторон индустриального развития территорий проживания коренных народов исследователи называют развитие инфраструктуры, возникновение новых рабочих мест, увеличение дохода местного населения и рост налоговых поступлений, но тут же отмечают риск исчезновения традиционных промыслов и иных элементов национальных культур, ведущего к утрате культурной идентичности (Živojinović et al., 2024). И действительно, развитие новых видов землепользования, в том числе добыча сырья для «зеленого сдвига» и других целей, а также производство электроэнергии, сопровождаемые строительством дорог и иной инфраструктуры, уже являются движущими факторами негативных изменений в традиционном оленеводстве в Фенноскандии (по мнению 60 % респондентов опроса, проведенного в рамках одного из исследований проекта Artic Hub) (Turunen et al., 2024). С учетом текущей геополитической ситуации горнодобывающая промышленность вызывает все больше споров – с одной стороны, ЕС стремится к самообеспечению себя необходимыми полезными ископаемыми, с другой – речь идет о возможном нарушении фундаментальных прав проживающих на соответствующих территориях граждан и несоблюдении исследовательской этики, что указывает на дальнейшее обострение «войны за ресурсы» не только между государствами, но и в будущем между государствами и населением Арктики, у которого растут недовольство превращением их земель в «Эльдорадо для крупных компаний» и ощущение отсутствия государственной защиты их законных прав и интересов (Suopajärvi et al., 2024). Необходимо понимать, что все перечисленные явления не проблема будущих поколений, в частности, метеорологические наблюдения в исландском Вестфирдире доказывают, что климат в последние несколько лет начал меняться быстрее и до конца столетия эта арктическая страна столкнется с соответствующими изменениями физической и антропогенной среды, а то, как быстро это произойдет, зависит от сокращения антропогенных выбросов (Bannan et al., 2022). Ученые также все чаще указывают на связь между повышением температур в Арктике и увеличением числа обращений за психологической помощью представителей коренного населения, развитие «экологической тревожности», обострения соластальгии и появления таких психологических состояний, как «климатическое и экологическое горе» в качестве реакций на глобальные негативные изменения окружающей среды, в том числе связанные с изменением землепользования (строительством шахт, железных дорог, ветряных электростанций и т. д.), а также отсутствием власти в принятии экологических решений в случаях, когда их права ограничиваются политическими решениями (Markkula et al., 2024). Речь также идет и о сохранении биобезопасности – вечная мерзлота является резервуаром биологических, химических и радиоактивных материалов, поэтому продолжающееся таяние ведет к пробуждению древних, зачастую неизвестных науке примитивных микроорганизмов, что повышает риск биологической опасности, в том числе и за пределами Арктики (Ali et al., 2024). Кроме того, таяние вечной мерзлоты, в том числе подводной, расположенной в морской среде,

способно вызвать выбросы в атмосферу еще одного парникового газа – метана (CH_4), содержащегося в естественных источниках региона (водно-болотных угодьях, пресноводных системах, газовых гидратах и т. д.) и образующегося в процессе повышения влажности почвы (Parmentier et al., 2024). Вкупе с увеличением частоты экстремальных погодных явлений эти негативные факторы уже повлекли за собой массовую гибель флоры и фауны, вызвали изменение миграции птиц и рыб, привели к нарушению прибрежных социально-экологических систем и уменьшению (а иногда и полному уничтожению) рыбных и иных морских промысловых ресурсов (Pecuchet et al., 2025). В контексте здоровья населения и дикой природы Арктики необходимо упомянуть и продолжающееся загрязнение региона ртутью (Hg)[6].

Термин «точка невозврата» начал звучать и в отношении Антарктики – ледяного щита планеты, содержащего более 60 % мировых запасов пресной воды, где изменения климата ведут к таянию ледников, распаду ледяного шельфа и, как следствие, к повышению уровня океана[7]. Откалывание ледниковых масс ведет к смешению вод и перераспределению тепла в океане, нарушая поставку питательных веществ в эвфотическую зону, а значит, и стабильность верхнего слоя океана вместе с доступностью света, необходимых для жизни планктона, что оказывает влияние на поглощение CO_2 (Meredith et al., 2022). Эксперименты показывают, что вместе с ростом температуры увеличивается скорость таяния ледяного покрова, что в будущем приведет к быстрому опреснению континентального шельфа (Mathiot & Jourdain, 2023). Данные явления в Антарктике не связаны с выбросами парниковых газов непосредственно на ее территории, но являются результатом глобальных изменений в атмосфере и океане, происходя с той же скоростью, что и, например, в Гренландии, где такая взаимосвязь установлена, но это не делает климатический прогноз более оптимистичным, и моделирование демонстрирует, что при сохранении текущей политики повышение уровня моря произойдет не менее чем на 42 см (Edwards et al., 2021). Негативное влияние на климат континента оказывают и экстремальные температурные явления (тепловые волны и морские тепловые волны), способные спровоцировать «каскад» экстремальных событий, таких как вызванное атмосферной рекой рекордное повышение температур в Восточной Антарктиде и полное разрушение шельфового ледника Конгер в 2022 г. (Siegert et al., 2023). При этом в Антарктике отсутствует коренное население, однако ее территории также ощущают на себе прямое воздействие антропогенной активности, связанное с научной и туристической деятельностью (появление неместных видов флоры и фауны, мобилизация загрязняющих веществ от свалок вследствие таяния снега и т. д.) (Hughes et al., 2021). При этом исследователи призывают обратить внимание на отсутствие необходимых нормативов и критериев, под которые должно подпадать загрязнение, вызванное повышением деятельности человека (Bargagli & Rota, 2024).

6 Why is mercury a concern in the arctic? AMAP. https://clck.ru/3NNXMK

7 EU. (2020). Identifying ice loss ‘tipping points’ in Antarctica. https://clck.ru/3NNXP2

1.1. Общие международные правовые основы обеспечения экологической безопасности и соблюдения прав коренных народов

Повестка дня Организации Объединенных Наций (далее – ООН) в области устойчивого развития до 2030 г. A/RES/70/1 в перечне Целей устойчивого развития (далее – ЦУР) выделяет необходимость принятия срочных мер по борьбе с изменением климата и его последствиями, достижение которых невозможно без выполнения обязательств, взятых на себя развитыми странами – участницами Рамочной конвенции ООН (далее – РКИК) об изменении климата, по достижению цели совместной мобилизации (Цель #13)[8], лежащей в основе всех нормативов по охране окружающей среды. А именно отчетность по антропогенным выбросам; развитие программ по смягчению изменений климата; содействие и сотрудничество в области технологий минимизации антропогенных выбросов; сотрудничество в принятии подготовительных мер с целью адаптации к последствиям изменения климата; учет связанных с изменением климата соображений при проведении соответствующей социальной, экономической и экологической политики и принятии мер; содействие и сотрудничество в полном, открытом и оперативном обмене научной, технологической, технической, социально-экономической и юридической информацией, связанной с климатической системой и изменением климата; проведение развитыми странами национальной политики и принятие соответствующих мер по смягчению последствий изменения климата путем ограничения своих антропогенных выбросов парниковых газов и защиты и повышения качества своих поглотителей и накопителей парниковых газов; предоставление новых и дополнительных финансовых ресурсов для покрытия всех согласованных издержек, вызываемых выполнением сторонами Конвенции, являющимися развивающимися странами, и другие обязательства, предусмотренные ст. 4[9]. В рамках РКИК также подписан ряд соглашений, включающих:

1. Киотский протокол (1998), ключевыми положениями которого являются обязательства по сокращению выбросов парниковых газов в атмосферу, в том числе CH_4 и CO_2, установление прозрачности в области антропогенных выбросов и установление ответственности с учетом особенностей экономического развития сторон[10].

2. Балийский план действий (2007), признающий факт глобального потепления доказанным и призывающий к развитию и усилению мер по борьбе с ним, в том числе технологических, финансовых и политических[11].

3. Копенгагенское соглашение (2009), в котором глобальное критическое изменение климата рассматривается как одна из главных проблем человечества, имеющая под собой научное обоснование и требующая срочного решения, для чего существует необходимость в сокращении антропогенных выбросов, активизации действий и международного сотрудничества в области снижения глобальных и национальных выбросов парниковых газов с поддержкой менее развитых стран более развитыми,

---

8 United Nations. (2015, October 21). Resolution adopted by the General Assembly on 25 September 2015. https://clck.ru/3NNZvD

9 Рамочная конвенция ООН об изменении климата. Принята 9 мая 1992 г. https://clck.ru/3NNZxc

10 ООН. (1998). Киотский протокол. https://clck.ru/3NNa4f

11 United Nations. (2007, December 14). FCCC/CP/2007/L.7/Rev.1. https://clck.ru/3NNa6R

а также в принятии мер по борьбе с вырубкой и деградацией лесных массивов, влекущих за собой снижение поглощения парниковых газов, сохранению биоразнообразия и условий жизни коренных народов[12].

4. Канкунские договоренности (2010), вновь направленные на повышение прозрачности в области ежегодных выбросов парниковых газов, а также их снижения в зависимости от экономического развития той или иной страны[13].

5. Дурбанская платформа (2011), предусматривающая продолжение действия Киотского протокола, а также устанавливающая структуру Зеленого климатического фонда, задачей которого является поддержка в адаптации к изменениям климата менее экономически развитых стран[14].

6. Парижское соглашение (2015), вновь поднимающее вопросы отчетности и прозрачности, призывающее к принятию реальных действий по выполнению обязательств, взятых на себя странами – участницами РКИК, принятию действий в рамках Киотского протокола, удержанию роста глобальной средней температуры на уровне значительно ниже 2 °C сверх доиндустриального уровня и стремлению к ограничению роста температуры до 1,5 °C сверх доиндустриального уровня, признавая в целях снижения рисков и последствий изменения климата[15].

К общим международным основам охраны экологической безопасности и прав коренных народов в полярных регионах также можно отнести:

1. Конвенцию о континентальном шельфе (1958), обязывающую прибрежные государства принимать в зоне безопасности все меры охраны морских живых ресурсов от вредоносного воздействия[16].

2. Международный пакт об экономических, социальных и культурных правах (1966), устанавливающий запрет на лишение народов принадлежащих им средств существования[17].

3. Конвенцию по предотвращению загрязнения моря сбросами отходов и других материалов (1975), направленную на эффективную борьбу с загрязнением морской среды и налагающую на страны-участницы обязательства по контролю за сбросами[18].

4. Конвенцию о трансграничном загрязнении воздуха на большие расстояния (1979), направленную на охрану человека и окружающей среды от загрязнения воздуха[19].

---

12 United Nations. (2009, December 18). FCCC/CP/2009/L.7. https://clck.ru/3NNa8z

13 United Nations. (2011, March 15). FCCC/CP/2010/7/Add.1. https://clck.ru/3NNaGB

14 Дурбанская платформа РКИК ООН. (2013, июль). https://clck.ru/3NNaHD

15 United Nations. (2015, December 12). FCCC/CP/2015/L.9/Rev.1. https://clck.ru/3NNaJE

16 Конвенция о континентальном шельфе. (1958). https://clck.ru/3NNaL3

17 ООН. (1966, 16 декабря). Международный пакт об экономических, социальных и культурных правах. https://clck.ru/3NNaM5

18 ООН. (1975). Конвенция по предотвращению загрязнения моря сбросами отходов и других материалов. https://clck.ru/3NNaNq

19 ООН. (1979). Конвенция о трансграничном загрязнении воздуха на большие расстояния. https://clck.ru/3NNaS5

5. Конвенцию ООН по морскому праву (1982), среди прочего оговаривающую право прибрежных государств принимать законодательные меры сохранения окружающей среды и предотвращения ее загрязнения[20].

6. Венскую конвенцию об охране озонового слоя (1985), основной целью которой является защита здоровья человека и окружающей среды от последствий изменения состояния озонового слоя, вызванных антропогенной активностью[21].

7. Конвенцию о коренных народах и народах, ведущих племенной образ жизни в независимых странах (1989), возложившую на страны-участницы обязанность содействовать полному осуществлению социальных, экономических и культурных прав коренных народов при уважении их социальной и культурной самобытности, а также в случае необходимости принимать специальные меры для охраны соответствующих народов, их институтов, труда, культуры и окружающей среды[22].

8. Конвенцию об оценке воздействия на окружающую среду в трансграничном контексте (1991), требующую от сторон принятия всех возможных мер по предотвращению значительного вредного трансграничного воздействия в результате планируемой деятельности и контроля за ним, такого как оценка воздействия на окружающую среду[23].

9. Конвенцию о биологическом разнообразии (1992), направленную на противодействие утрате биологического разнообразия планеты, признающую зависимость коренных народов от биологических ресурсов и необходимость совместного их использования на справедливой основе, а также закрепляющую за странами-участницами обязанность создания особо охраняемых территорий, принятию мер по реабилитации и восстановлению находящихся в опасности видов и взаимодействию в этих целях с коренными народами на принципах уважения, сохранения и поддержки их знаний и традиций[24].

10. Декларацию Организации Объединенных Наций о правах коренных народов (2007), запрещающую любые действия, направленные на лишение коренных народов их земель, территорий и ресурсов, в том числе действия, результатом которых может быть уничтожение культуры и самобытности. Коренные народы при этом наделяются правом на участие в принятии решений по вопросам, которые затрагивали бы их права[25].

11. Стокгольмскую конвенцию о стойких органических загрязнителях (2011), признающую особую уязвимость экосистем и общин в Арктике вследствие биоусиления воздействия стойких органических загрязнителей и заражения используемых коренными народами традиционных пищевых продуктов и требующую

---

20 ООН. (1994). Конвенция ООН по морскому праву. https://clck.ru/3NNaVL

21 ООН. (1985). Венская конвенция об охране озонового слоя. https://clck.ru/3NNaa2

22 ООН. (1989). Конвенция о коренных народах и народах, ведущих племенной образ жизни в независимых странах. https://clck.ru/3NNabb

23 ООН. (1991). Конвенция об оценке воздействия на окружающую среду в трансграничном контексте. https://clck.ru/3NNadD

24 ООН. (1992). Конвенция о биологическом разнообразии. https://clck.ru/3NNmeG

25 ООН. (2008, 17 марта). Декларация ООН о правах коренных народов. https://clck.ru/3NNccN

принятия мер по сокращению или ликвидации выбросов в результате антропогенной активности[26].

12. Минаматскую конвенцию о ртути (2013), цель которой – охрана здоровья человека и окружающей среды от антропогенных выбросов и высвобождений ртути и ее соединений[27].

Сюда же входят международно-правовые инструменты, принятые Международной морской организацией (далее – ИМО), такие как Международная конвенция по предотвращению загрязнения с судов МАРПОЛ 73/78 (направлена на борьбу с загрязнением океана), Международный кодекс по безопасности для судов, использующих газы или иные виды топлива с низкой температурой вспышки (кодекс МГТ 2017), Международная конвенция о контроле судовых балластных вод и осадков и управлении ими (2004) и др. ИМО также занимается разработкой среднесрочных мер по сокращению выбросов парниковых газов с судов и использования водорода и аммиака в качестве судового топлива[28].

1.2. Специальные международные правовые основы обеспечения безопасности и соблюдения прав коренных народов в Арктике и Антарктике

Учитывая стратегические, социальные, экономические и климатические особенности полярных регионов, на сегодняшний день сформирована обширная многоуровневая международная правовая база обеспечения безопасности на их территории. Помимо общих международных правовых основ обеспечения экологической безопасности и охраны прав и законных интересов коренных народов, разработан целый пласт международных актов, направленный на модификацию национальных законодательств, развитие всестороннего международного сотрудничества и повышение принципов прозрачности в области антропогенных выбросов непосредственно в Арктике и Антарктике. В рамках настоящего исследования основными специальными международными правовыми актами, обеспечивающими безопасность в указанных регионах, являются:

1. Договор об Антарктике (1959), запрещающий ядерные взрывы в Антарктике и удаление в этом районе радиоактивных материалов, устанавливающий принципы прозрачности работы и научных исследований, установление контроля за экспедициями и станциями, а также призывающий к сотрудничеству в области разработки мер охраны и сохранения живых ресурсов в Антарктике[29].

2. Протокол об охране окружающей среды к Договору об Антарктике (1991), согласно которому его стороны берут на себя ответственность за «всеобъемлющую охрану окружающей среды Антарктики и зависящих от нее и связанных с ней экосистем»[30], в связи с чем признается необходимым ограничение отрицательных воздействий на окружающую среду Антарктики и зависящих от нее и связанных с ней эко-

---

26 Стокгольмская конвенция о стойких органических загрязнителях. (2001). https://clck.ru/3NNcdR

27 ООН. (2013). Минаматская конвенция о ртути. https://clck.ru/3NNchn

28 Международная морская организация. Официальный интернет-ресурс Министерства транспорта Российской Федерации. https://clck.ru/3NNcjJ

29 Договор об Антарктике. (1959). https://clck.ru/3NNck5

30 Протокол об охране окружающей среды к Договору об Антарктике. https://clck.ru/3QHnur

систем (отрицательное влияние на климат, погоду, качество воды и воздуха, ледовую и морскую среды, флору и фауну)[31].

3. Декларация защиты окружающей среды Арктики (1991), направленная на сохранение окружающей среды и природных ресурсов, установление мониторинга ее состояния и сокращение загрязнений, а также согласование принципов природоохраны с потребностями коренного населения[32].

4. Договор о согласии и сотрудничестве между Российской Федерацией и Канадой (1992), подчеркивающий роль стран-участниц в сохранении окружающей среды и направленный в том числе на укрепление их сотрудничества в Арктике, что рассматривается как приоритетная область российско-канадских отношений. Договор также предполагает постоянное взаимодействие с коренными народами северных регионов[33].

5. Российско-шведская декларация (1993), закрепляющая международное сотрудничество между Российской Федерацией и Швецией, подразумевающее «социально и экологически ориентированную политику, экономическую либерализацию, свободу торговли и предпринимательства в рамках цивилизованного отношения к окружающей среде и рационального использования природных ресурсов»[34].

6. Первая Киркенесская декларация (1993), установившая основные принципы взаимодействия в Баренцевом/Евроарктическом регионе и учредившая Совет Баренцева/Евроарктического региона. Декларация подчеркивала важность научной и технологической кооперации в регионе, развития культурных отношений и поддержки коренных народов (ненцев и саамов), для чего было предложено создать специальную рабочую группу[35].

7. Декларация об основах отношений между Российской Федерацией и Королевством Норвегия (1996), направленная на плодотворное взаимодействие в Баренцевом/Евроарктическом регионе, укрепление уважения прав человека и его основных свобод, включая права национальных меньшинств, интенсификацию работы по глобальным вопросам окружающей среды и решение проблем, связанных с внутренней зависимостью между энергетикой, охраной окружающей среды и экономическим развитием[36].

8. Икалуитская декларация (1998), страны-участницы которой приняли на себя обязательства по улучшению благосостояния жителей Арктики, а также принятию мер по защите и улучшению окружающей среды, экономики, культуры и здоровья коренных народов и других народов, проживающих в регионе[37].

---

31 Протокол об охране окружающей среды. (1991). https://clck.ru/3NNcm2

32 Декларация о защите окружающей среды в Арктике. https://clck.ru/3NNcpo

33 Договор о согласии и сотрудничестве между Российской Федерацией и Канадой. (1993). https://clck.ru/3NNcs3

34 Российско-шведская декларация. (1993). https://clck.ru/3NNct2

35 Declaration Cooperation in the Barents Euro-Arctic Region. (1993, January 11). https://clck.ru/3NNcut

36 Декларация об основах отношений между Российской Федерацией и Королевством Норвегия. (1996). https://clck.ru/3NNcwu

37 Икалуитская декларация. (1998). https://clck.ru/3NNcyX

9. Инувикская декларация об изменении арктического климата и глобальных действиях (2005), призывающая к объединению человечества в целях резкого сокращения антропогенных выбросов для предотвращения дальнейших критических изменений климата, где Арктика – один из ключевых компонентов климатического благополучия планеты. Декларация также признает, что текущие изменения климата представляют собой экзистенциальную угрозу безопасности коренных жителей Арктики[38].

10. Илулиссатская декларация (2008), утверждающая уникальный статус Дании, Канады, России, США, Норвегии и Канады как государств, способных найти решение климатического кризиса в Арктике, для чего нет необходимости в разработке специального правового режима для Северного Ледовитого океана – достаточно существующих норм международного права и национальных нормативных правовых актов стран-участниц, но лишь при условии их дальнейшего всестороннего сотрудничества[39].

11. Декларация инуитов циркумполярного региона о суверенитете в Арктике (2009), от имени проживающих на территории Гренландии, Канады, США и России инуитов напоминающая государствам, что «в погоне за экономическими возможностями в продолжающей теплеть Арктике» необходимо в том числе стремиться к экологической устойчивости, недопущению пагубной эксплуатации ресурсов и предотвращению маргинализации коренного населения[40].

12. Нуукская Декларация об окружающей среде и развитии в Арктике (2010), напоминающая, что инуиты – один народ, проживающий на территориях четырех различных стран, но объединенный уважительным отношением к разделению культуры, ресурсов и «самой жизни» с другими народами, и признающая факт того, что права коренных народов, в том числе инуитов, наряду с фундаментальными правами человека до сих пор до конца не реализованы, документ указывает на хрупкость окружающей среды Арктики в условиях все большей разработки наземных и водных ресурсов и призывает к обмену знаниями с коренным населением и более активному участию последнего в вопросах охраны территорий, на которых оно проживает[41].

13. Декларация по итогам встречи глав правительств стран – членов СБЕР (2013), подтверждающая приверженность стран-участниц принципам Первой Киркенесской декларации и акцентирующая внимание на охране окружающей среды и защите прав коренного населения, в том числе права участвовать в процессе принятия решений по вопросам, затрагивающим их права, а также права коренных народов на сохранение традиционного образа жизни, включая занятие охотой, рыболовством и оленеводством[42].

14. Международный кодекс для судов, эксплуатирующихся в полярных водах (Полярный кодекс 2014), принятый в целях повышения безопасности эксплуатации судов и ограничения ее влияния на людей и окружающую среду, в своей Преамбуле признающий, что «сообщества прибрежных народов Арктики могут быть, а полярные экосистемы являются уязвимыми в отношении такой деятельности человека,

---

38 The Inuvik Declaration. (2008, December 5). https://clck.ru/3NNd5z

39 The Ilulissat Declaration. (2008, May 27–29). https://goo.su/vuqV

40 A Circumpolar Inuit Declaration on Sovereignty in the Arctic. (2009). https://clck.ru/3NNdEn

41 Nuuk Declaration. (2010). https://clck.ru/3NNdFu

42 Декларация по итогам встречи глав правительств стран – членов СБЕР. (2013). https://clck.ru/3NNdGr

как судоходство», а в Части II-A устанавливающий меры по предотвращению загрязнения (эксплуатационные и конструкционные требования)[43].

15. Рейкьявикская декларация (2021), признающая неразрывную связь между здоровьем человека, животными и окружающей средой и говорящая о необходимости дальнейшего развития сотрудничества в области безопасности и здоровья арктических сообществ и социального благополучия жителей Арктики, а также призывающая к продолжению исследований в области новых, возникающих и регулируемых загрязнителей и усилению мер по реализации обязательств, связанных с загрязнениям ртутью (Hg) и триоксидом углерода (CO_3)[44].

16. Илулиссатская декларация (2022), подтверждающая статус и цели Приполярного совета инуитов, признающая вступление инуитов и остального человечества в эпоху экологической и глобальной небезопасности и осуждающая угрозы продовольственной безопасности, изменений в дикой природе, а также экологическое и промышленное воздействие на территории проживания инуитских общин[45].

17. Хельсинкская декларация об изменении климата в Антарктике (2023), признающая, что в случае сохранения выбросов CO_2 на текущем уровне атмосфера и океаны будут продолжать нагреваться, а океаны – закисляться. Декларация еще раз подтверждает, что добыча ископаемых на континенте в любых целях, кроме научных исследований, запрещена, а также говорит о необходимости совместной работы по изучению воздействия глобального изменения климата на Антарктику, а также роли самой Антарктики и Южного океана в регулировании глобального климата и будущего повышения уровня моря[46].

Центральной организацией сотрудничества в Арктике является учрежденный в 1996 г. арктическими государствами (Россия, Дания, Норвегия, Швеция, Финляндия и Канада) Арктический совет (далее – АС), целями которого являются охрана окружающей среды и устойчивое развитие региона[47]. Имеющий форму Межправительственного форума АС включает в себя шесть постоянных участников, представляющих интересы коренных народов Арктики: Алеутскую международную ассоциацию, Арктический совет атабасков, Международный совет гвичинов, Инуитский приполярный совет, Союз саамов и Ассоциацию коренных малочисленных народов Севера, Сибири и Дальнего Востока РФ. При АС также действуют специальные рабочие группы, такие, например, как Международная организация «Программа арктического мониторинга и оценки» (AMAP) (Arctic Monitoring and Assessment Programme (AMAP)), занимающаяся оценкой состояния арктической окружающей среды, и «Защита арктической морской среды» (ПАМЕ) (Protection of the Arctic Marine Environment (PAME)), в чьи задачи входит исследование вопросов политики и разработка мер, связанных с охраной морской среды[48]. Кроме АС, действующими организациями являются: 1) Международный Баренцев

---

43 Международный кодекс для судов, эксплуатирующихся в полярных водах (Полярный кодекс). (2014). https://clck.ru/3NNdQw

44 Рейкьявикская декларация. (2021). https://clck.ru/3NNdST

45 Приполярный совет инуитов. Илулиссатская декларация 2022 года. (2022). https://clck.ru/3NNdV3

46 Хельсинкская декларация об изменении климата и Антарктике. (2023). https://clck.ru/3NNdXN

47 Арктический совет. https://clck.ru/3NNdZC

48 Арктик-фонд. Международные программы AMAP, AEPS, CAFF, PAME. https://clck.ru/3NNdaX

секретариат, учрежденный в рамках Соглашения между правительствами Финляндской Республики, Королевства Норвегия, Российской Федерации и Королевства Швеция о создании Международного Баренцева секретариата в целях развития сотрудничества в Баренцевом/Евроарктическом регионе[49]; 2) учрежденный в 1998 г. Совет Баренцева/Евроарктического региона (далее – СБЕР), среди целей которого в том числе взаимодействие в области охраны окружающей среды и улучшения положения коренного населения Севера[50]; 3) Баренцев региональный совет (далее – БРС), являющийся самостоятельным органом многостороннего сотрудничества 13 административно-территориальных образований Баренцева региона, в состав которого входят их руководители и представители коренных народов (саамов, вепсов и ненцев)[51]; 4) независимая Рабочая группа по вопросам коренных народов в статусе постоянного консультационного органа при СБЕР и БРС[52]. На сегодняшний день Российская Федерация денонсировала Соглашения между Правительствами Финляндской Республики, Королевства Норвегия, Российской Федерации и Королевства Швеция о создании Международного Баренцева секретариата в целях развития сотрудничества в Баренцевом/Евроарктическом регионе (Распоряжение Правительства РФ № 921-р от 16.04.2025[53]) и была исключена из СБЕРа, который также покинула и Финляндия[54].

В Антарктике роль специального международного органа выполняет Секретариат Договора об Антарктике, при котором создан Комитет по охране окружающей среды, функциями которого являются представление соображений и формулирование рекомендаций Сторонам в связи с осуществлением Протокола по охране окружающей среды, включая действие его Приложений, для рассмотрения на Консультативных совещаниях по Договору об Антарктике (ст. 11 Протокола по охране окружающей среды)[55].

2. Роль Арктики и Антарктики в обеспечении развития и функционирования центров обработки данных

За последние несколько лет в Арктике был реализован целый ряд успешных проектов по размещению в регионе центров обработки данных (далее – ЦОД), превратив последние в новый тип критической инфраструктуры, основной причиной чему послужили обильные запасы электроэнергии, в том числе зеленой, и ее низкая цена вкупе с холодным климатом, наличием оптоволоконного подключения и разумными

---

49 Соглашение между Правительством Финляндской Республики, Правительством Королевства Норвегия, Правительством Российской Федерации и Правительством Королевства Швеция. (2007). https://clck.ru/3NNdhK

50 Совет Баренцева/Евроарктического региона (СБЕР). (2021, 1 июля). https://clck.ru/3NNdic

51 Баренцев региональный совет. (2021, 2 июля). https://clck.ru/3NNdjX

52 Совет Баренцева/Евроарктического региона (СБЕР). (2021, 1 июля). https://clck.ru/3NNdmL

53 Распоряжение Правительства РФ № 921-р от 16.04.2025. (2025). https://clck.ru/3NNdnn

54 Кабмин денонсировал соглашение о сотрудничестве в Баренцевом регионе. (2025, 18 апреля). ТАСС. https://clck.ru/3NNdob

55 Протокол об охране окружающей среды к Договору об Антарктике от 4 октября 1991 года. (1998). https://clck.ru/3NNdpS

ценами на землю (Saunavaara & Laine, 2021). Так, например, Исландия позиционирует себя как идеальное место для строительства ЦОД благодаря своей дешевой зеленой энергетике, стремясь стать крупнейшим оператором центров обработки данных в странах Северной Европы[56]. И действительно, оценивая перспективы этой страны для развития ЦОД-индустрии, международная аудит-консалтинговая корпорация КПМГ среди ее преимуществ выделила возможность использования естественного охлаждения (системы вентиляции без дополнительных охладителей) и достаточно низких цен на электроэнергию (при этом рост энергопотребления в Исландии уже в 2018 г. в среднем составлял 75 % за пятилетний период)[57]. Рост запросов на строительство и расширение уже существующих ЦОД продолжает расти вместе с увеличением проектов с использованием технологий ИИ и количеством данных, требующих обработки; в частности, Verne в Исландии принадлежит работающий на гидро- и геотермальной энергии ЦОД, который, по заявлениям компании, «не наносит никакого ущерба планете», но в то же время использует технологии жидкостного охлаждения[58] (примечательно, что на своей официальной странице Verne не уточняют, какое именно жидкостное охлаждение используется – непрямого водяного, иммерсионного с использованием специального минерального масла или какой-то иной технологии). Заслуживает внимания и запланированный, но так и не возведенный из-за изменений в норвежском законодательстве по отношению к майнерам ЦОД Kolos, который должен был быть расположен непосредственно в Арктике – норвежском Баллангене. Заявленный как самый большой в мире, он расположился бы на 600 000 кв. м и использовал климатическое охлаждение, функционируя на гидроэнергии[59]. Стремясь к прозрачности и повышению доверия, Норвежская ассоциация индустрии центров обработки данных (Norsk Datasenterindustri) представила отчет по ЦОД за 2023–2024 гг., в котором еще раз подчеркнула: рост данной индустрии обусловлен цифровизацией и повсеместным внедрением искусственного интеллекта, что является причиной дополнительных выбросов CO_2 (на 2024 г. в Великобритании и Германии данные выбросы были в 12 раз больше, чем в Норвегии), и подтвердила важность ЦОД для экономики страны, также напомнив, что в королевстве данная индустрия была взята под контроль посредством внесения изменений в Закон «Об электронных коммуникациях»[60]. Не отстает и Финляндия, ставшая местом размещения ЦОД компании Meta[61]. В том числе один из их ЦОД, обрабатывающий колоссальные объемы данных, размещен в лапландском Лулео, где, по заявлениям самой компании, достигнута цель нулевых выбросов CO_2 посредством использования «чистой и возобновляемой энергии» и стратегии добавления

56 Moss, S. (2024, 26 March). Iceland's AI moment. https://clck.ru/3NNeJD

57 The Icelandic Data Center Industry. (2018, March). https://clck.ru/3NNeLi

58 High-performance computing in Iceland. Verne. https://clck.ru/3NNeNQ

59 Kolos Data Center. https://clck.ru/3NNoHk

60 The Data Center Industry in Norway 2023–2024. (2024). Norwegian Data Center Industry. https://clck.ru/3NNeX4

61 Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

возобновляемых источников энергии в локальную сеть, более того, к 2030 г. компания будет «восстанавливать больше воды, чем потреблять»[62].

В России как некоммерческие, так и коммерческие ЦОД также продолжают расти. Непосредственно за полярным кругом на земельном участке площадью 15 тыс. кв. м в скором времени будут размещены технологические модули общей емкостью 4 000 устройств производительностью 16 МВт, входящие в ЦОД, принадлежащий резиденту Арктической зоны РФ – компании «Интелион Север»[63]. Государственная корпорация «Росатом» в попытке избежать влияния санкций также планирует запуск ЦОД в Мурманской области – на базе Кольской атомной электростанции, около 20–25 % электроэнергии которой остаются невостребованными, в то время как холодный климат позволяет не устанавливать системы охлаждения, что также снизит расходы электроэнергии[64]. Российский хостинг-провайдер RUVDS пошел еще дальше и запустил в 2024 г. модульный ЦОД на дрейфующей льдине, работающий на дизель-генераторах, непосредственно рядом с Северным полюсом в рамках эксперимента, который был завершен в течение месяца из-за появления трещины на льдине[65]. Аналогичный проект RUVDS запланировал на 2025 г., но на этот раз ЦОД будет размещен на Южном полюсе[66].

Чили, стремящаяся также стать страной, привлекающей операторов ЦОД, планирует протянуть подводные кабели к последнему из континентов, лишенному их, – в Антарктику. Antarctic SMART Cable, обладающий почти неограниченной пропускной способностью, должен соединить крупнейший исследовательский центр Антарктиды либо с американской станцией Мак-Мердо, либо с новозеландским Инверкаргиллом, либо с австралийским Сиднеем, что может улучшить текущие и будущие исследования Антарктики, а также создать возможность стабильного взаимодействия для ученых и персонала[67].

3. Риски, связанные с ростом индустрии ЦОД, и попытки их нивелировать

К первой группе рисков, связанных со строительством ЦОД в арктических странах и Антарктике, безусловно, относятся риски, связанные с их негативным влиянием на окружающую среду. Норвежский исследовательский центр SINTEF Energi AS обращает внимание на то, что, когда для охлаждения ЦОД используется электроэнергия (воздушное охлаждение процессоров данных), генерируется избыточное количество

---

62 Meta's* Luleå Data Centre. https://clck.ru/3NNedg (* Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации)

63 Первый коммерческий ЦОД в Мурманской области запустит с господдержкой резидент АЗРФ. (2023, 13 июля). Корпорация развития Дальнего Востока и Арктики. https://clck.ru/3NNeje

64 ЦОД «Арктика» на Кольской АЭС построят полностью на российском оборудовании. (2022, 18 июля). ТАСС. https://clck.ru/3NNeoC

65 Первый ЦОД в Арктике! RuVDS. https://clck.ru/3NNepL

66 RUVDS проведет испытания серверного оборудования в Антарктиде. (2024, 16 октября). RuVDS. https://clck.ru/3NNeqT

67 Winston Qiu. (2024, December 14). US NSF Requests for Information on Antarctic SMART Cable. Submarine cable networks. https://clck.ru/3NNevG

тепла температурой 40–50 °C, эта температура увеличивается до 60–80 °C, если используются более эффективные системы охлаждения (жидкостное или двухфазное, при использовании которого жидкий хладагент испаряется в холодном пластинчатом теплообменнике), но в обоих случаях данное избыточное тепло, как правило, никак не используется, более того, выбросы CO_2 от ЦОД уже сейчас составляют не менее 2 % от мировых, что эквивалентно ущербу от авиационной индустрии[68]. Избыточное тепло, если оно обладает достаточно высокой температурой, можно использовать для обогрева зданий и иных промышленных и бытовых целей, как это делается, например, в Швеции (Yuan et al., 2023). Тем не менее на сегодняшний день избыточное тепло чаще всего выбрасывается в атмосферу, на что, например, обращают внимание специалисты PivIT Global (компания занимается обслуживанием и ремонтом ЦОД), напоминая, что избыточное тепло не может быть использовано для обогрева домов и зданий, если ЦОД находится в отдаленном и/или малонаселенном регионе, кроме того, такая утилизация требует создания дорогостоящей инфраструктуры[69]. Помимо избыточного тепла, в атмосферу выбрасываются такие парниковые газы, как CO_2, CH_4 и N_2O (закись азота), что связано как непосредственно с функционированием, так и со строительством ЦОД, где особую угрозу для окружающей среды представляют утечки хладагентов, используемых в системах охлаждения, нельзя также забывать и об использовании дизельных генераторов, запускаемых в случаях отключения основной электроэнергии либо во время тестирования оборудования, которое происходит на регулярной основе, и о колоссальном расходе воды, учитывая, что большинство действующих ЦОД используют испарительное охлаждение, выделяющее тепло в окружающую среду (Thangam et al., 2024). Так, согласно официальным данным, предоставленным Google в отчете, общий объем парниковых выбросов, связанный с их деятельностью, вырос только в 2023 г. на 48 % по сравнению с 2019 г.[70] Еще менее оптимистично выглядят результаты независимых расследований – британский Guardian представляет собственный анализ, согласно которому выбросы ЦОД, принадлежащих таким технологическим гигантам, как Google, Microsoft , Meta[71] и Apple, с 2020 по 2022 г. могли быть на 662 % выше официально зарегистрированных, а заниженные показатели являются следствием несовершенств систем учета и сертификации[72].

Ситуация усугубляется тем, что в той же Норвегии технологии развиваются быстрее, чем их правовое регулирование[73]. В попытке взять функционирующие в королевстве ЦОД под контроль, норвежский законодатель дополнил Закон «Об электронных коммуникациях» положениями ст. 3–7, включивших требование обязательной регистрации операторов ЦОД и рекомендацию использовать

---

68 Foslie, S. St. & Moen, O. M. (2021, March 16). This is how we reduce data centres carbon footprint. SINTEF. https://clck.ru/3NNkPD

69 4 Ways Data Center Heat Can Be Reused. (2024, March 26). Pivit Global. https://clck.ru/3NNkN7

70 Google Environmental Report 2024. https://clck.ru/3NNkM4

71 Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

72 Data center emissions probably 662 % higher than big tech claims. Can it keep up the ruse? (2024, September 15). https://clck.ru/3NNkL8

73 Andreassen, B. L. (2023, April 28). Scandinavian data centres: fewer jobs and less profit than forecast. Nordic Labour Journal. https://clck.ru/3NNkKJ

«наилучшие доступные технические решения, признанные стандарты, стоимость и полезность применяемых мер»[74]. Можно предположить, что речь идет о следующих общепризнанных стандартах и сертификатах, применимых к ЦОД:

1. ISO 14001 – международно признанный стандарт для систем экологического менеджмента, способствующий достижению ЦУР ООН по защите климата, развитию ответственного потребления и производства, созданию доступной и чистой энергии и др.[75] Данный международный стандарт определяет требования к системе экологического менеджмента, которую организация может использовать для улучшения своих экологических показателей, что включает развитие экологической политики организации, оценку влияния на окружающую среду, противодействие загрязнению окружающей среды, оценку потенциальных рисков и стремление к постоянному улучшению показателей экологической эффективности[76].

2. ISO 50001 – международно признанный стандарт, предполагающий интеграцию управления энергопотреблением в общие усилия сертифицируемой компании по улучшению экологического менеджмента[77].

3. LEED – международно признанная система оценки экологичности всех типов построек, в основе которой лежит решение проблемы изменения климата (защита и восстановление водных ресурсов, защита биоразнообразия, снижение негативного влияния на климат планеты и пр.) и достижение ЦУР ООН[78].

4. EU DC CoC – Европейский кодекс поведения для центров обработки данных, являющийся добровольной инициативой, разработанной Объединенным исследовательским центром и направляющий владельцев и операторов ЦОД «в экономически эффективном снижении потребления энергии без ущерба для критически важной функции их объектов»[79].

5. BREEAM – международно признанный сертификат оценки экологической устойчивости зданий, где конечная цель – нулевые выбросы CO_2 к 2050 г.[80]

6. Nordic Swan Ecolabel – международно признанный сертификат, основанный на оценке полного жизненного цикла продукта, цель которого – снизить воздействие на окружающую среду в процессе производства и потребления товаров[81]. Непосредственно сами ЦОД не относятся ни к одной из сертифицируемых Nordic Swan Ecolabel групп, однако к ним относятся используемые в строительстве и обслуживании материалы, а также офисы, находящиеся на территории ЦОД[82].

7. EKOenergy label – международно признанный сертификат возобновляемых электроэнергии, тепла, газа и охлаждения, включающий ежегодный аудит, проверяющий факт соответствия проданных или использованных объемов электроэнергии

74 Ekomloven. (2024). Lovdata. https://clck.ru/3NNk43

75 ISO 14001:2015. https://clck.ru/3NNk5U

76 Environmental management systems – Requirements with guidance for use. https://clck.ru/3NNk6e

77 ISO 50001. https://clck.ru/3NNk7h

78 LEED rating system. https://clck.ru/3NNkB7

79 EU. European Code of Conduct for Energy Efficiency in Data Centres. https://clck.ru/3NNkDm

80 Achieve your net zero goals with BREEAM certification. https://clck.ru/3NNkEs

81 Why choose ecolabelling? Nordic Swan Ecolabel. https://clck.ru/3NNkGq

82 Criteria. Nordic Swan Ecolabel. https://clck.ru/3NNjgb

с маркировкой требованиям, перечисленным в критериях EKOenergy (расположение солнечных панелей и ветряных турбин, геотермальных и морских установок за пределами охраняемых природных территорий, а также производство гидроэлектроэнергии с учетом миграции рыб и сохранением мест обитания водных видов и т. д.)[83].

9. ASHRAE – международные рекомендации по отоплению, охлаждению и кондиционированию воздуха[84].

10. Carbon Trust – международно признанный сертификат, направленный на снижение эксплуатационных выбросов и парниковых газов, требующий от компаний постоянного финансирования соответствующих изменений и раскрытия информации об их внедрении[85].

11. Положения нормативных актов Европейского союза, таких как Регламент Комиссии ЕС 2019/424 от 15 марта 2019 г., устанавливающий требования к экологическому проектированию серверов и устройств хранения данных в соответствии с Директивой 2009/125/ЕС Европейского парламента и Совета ЕС[86].

В то же время в национальных законодательствах появился тренд на смягчение требований. Так, к примеру, США планируют ослабить для ЦОД экологические ограничения на отдельных участках федеральной земли, где будут построены специальные электростанции, работающие на природном газе, обслуживающие массивные ЦОД, потребляющие не менее 1 ГВ электроэнергии (соответствует количеству энергии, потребляемой городом с населением в 10 000 000 человек)[87], соответствующий приказ был подписан президентом Джо Байденом в январе 2025 г.[88] В правовом авангарде здесь находится Россия – принятый Министерством строительства РФ свод правил СП 541.1325800.2024 «Здания и сооружения центров обработки данных. Правила проектирования» в обеспечение соблюдения требований Федерального закона от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений» и с учетом требований федеральных законов от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности», от 23 ноября 2009 г. № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации», установил обязательные общие требования к соблюдению санитарно-эпидемиологических и экологических требований по охране здоровья людей, окружающей природной среды и прилегающей застройки, энергосбережению и безопасности, а также к основным инженерно-техническим системам электро- и холодоснабжения[89].

---

83 The EKOenergy ecolabel. EKOenergy. https://goo.su/GWlE2

84 Updated and Improved Standards Review Database. ASHRAE. https://clck.ru/3NNjkf

85 Net Zero transition planning and delivery. Carbon Trust. https://clck.ru/3NNjno

86 EU. (2019). Document 32019R0424. https://clck.ru/3NNjrF

87 Biden plan would encourage AI data centers on federal lands. (2024, December 19). The Washington Post. https://clck.ru/3NNjsv

88 Biden Wants Data Centers, Clean Energy on Federal Land by 2027. https://clck.ru/3NNjuN

89 Приказ Министерства строительства РФ. СП 541.1325800.2024 от 23.12.2024. (2024). https://clck.ru/3NNje3

К экологическим рискам следует отнести и изменение землепользования, связанное со строительством, функционированием и обеспечением ЦОД электроэнергией. Строительство ЦОД и сопутствующей инфраструктуры предполагает вырубку леса на больших территориях, а также забор воды, часто питьевой, что может привести к необратимым экологическим последствиям (Thangam et al., 2024). Зеленая же энергетика также предполагает активное вмешательство в природный ландшафт от установки ветряных турбин и солнечных панелей до бурения глубоких скважин, как, например, это делает Исландия, где спрос на электроэнергию выше, чем она может предложить, и где разработан Проект исландского глубокого бурения (IDDP), предполагающий увеличение количества глубоких скважин с целью роста производства геотермальной энергии[90].

Наконец, к экологическим рискам относятся и проекты по расположению глубоководных морских кабелей. Весь жизненный цикл такого кабеля, включающий этапы установки, обслуживания и вывода из эксплуатации, связан с воздействием на окружающую среду, в том числе: нарушением среды обитания видов, химическим и шумовым загрязнением, изменением электромагнитных полей, тепловыделением и другими видами ущерба экологии (Taormina et al., 2018). Было бы несправедливо утверждать, что прокладка и эксплуатация глубоководных морских кабелей никак не урегулированы, но тем не менее вопросам защиты самих кабелей национальное и международное право уделяют гораздо больше внимания, чем вопросам охраны окружающей среды в районах, где они проложены. Так, ст. 79 Конвенции ООН по морскому праву (1982) наделяет все страны правом прокладывать подводные кабели и трубопроводы на континентальном шельфе при условии соблюдения «разумных мер для разведки континентального шельфа, разработки его природных ресурсов и предотвращения, сокращения и сохранения под контролем загрязнения», обязывая учитывать ранее проложенные кабели и трубопроводы, дабы не ухудшить возможности их ремонта и обслуживания[91]. На положениях этой статьи выстроено, например, внутреннее регулирование США, где выдачей разрешений на прокладку подводных кабелей занимается Национальная ассоциация безопасности на море, в том числе разрешение может быть выдано и на размещение подводного кабеля на территориях национальных морских заповедников[92].

Второй группой рисков, связанных с ростом индустрии ЦОД в арктических странах, являются социальные риски. Добыча необходимых для функционирования ЦОД металлов и минералов, непосредственная застройка и сопряженные с ней рубки, строительство дорог на местах пастбищ и землях, представляющих культурную ценность для проживающих там коренных народов, строительство гидро- и иных электростанций являются продолжением эксплуатационных практик, в том числе по отношению к проживающим в арктических регионах саамам – правовая защита их пастбищ, как и реализация их прав как коренного народа, зачастую имеет лишь номинальный характер и сводится к нулю с ростом потребности в зеленой электроэнергии и строительством ЦОД, в то время как сами саамы вновь сталкиваются

90 Moss, S. (2024, March 26). Iceland's AI moment. DCD. https://clck.ru/3NNjbz

91 Конвенция ООН по морскому праву. (1982). https://clck.ru/3NNjaX

92 Submarine Cables – Domestic Regulation. NOAA. https://clck.ru/3NNjXA

с таким наследием прошлого, как изъятие земель и даже насильственное переселение, где ярким примером служит ранее упомянутый ЦОД в Лулео, расположенный на пастбище саамских оленеводов, строительство которого с ними даже не обсуждалось[93]. На данную проблему уже обратили внимание в ООН, призвав учитывать права коренных народов при разработке месторождений «критически важных минералов», сопряженной с вырубкой лесов, загрязнением воды и почвы, потерей биоразнообразия и вынужденным переселением коренного населения[94]. Обещания создать большое количество рабочих мест в местах проживания коренных народов и отдаленных районах размещений ЦОД тоже не всегда соответствуют действительности – вместо 30 000 рабочих мест в Лулео было создано всего 56[95]. С ухудшением условий жизни сталкиваются и другие представители местного населения. Среди причин можно назвать рост цен – например, в привлекательной своей дешевой и избыточной электроэнергией Норвегии из-за роста цен на электричество уже пришлось закрыть теплицы в ряде регионов[96]. Все это приводит к росту протестов против строительства ЦОД по всему миру и, разумеется, в Северной Европе как точке их сосредоточения – граждане полагают, что нарушаются их права и законные интересы, снижается качество жизни, а земли отдаются иностранным технологическим компаниям в приоритетном порядке[97].

Заключение

Полученные результаты демонстрируют, что строительство ЦОД и развитие сопутствующей их функционированию и обслуживанию индустрии в Арктике и Антарктике сопряжены с особыми рисками, которые определены их географическим расположением, уязвимостью биологического разнообразия и этническим составом населения. Данные риски делятся на две основные группы: экологические и социальные. Экологические риски связаны с тем, что темпы и масштабы происходящих в них изменений не позволяют местным экологическим системам своевременно адаптироваться, а будущие изменения не поддаются адекватной количественной оценке (Robinson, 2022). В то же время малейшие колебания температур в их регионах, как и повышение антропогенной активности, способны вызвать цепную реакцию необратимых климатических, социологических и экономических изменений на всей планете[98]. В зоне риска, таким образом, оказывается биологическая, продовольственная и непосредственно физическая безопасность человечества. Социальные же риски связаны с индустриальным развитием

93 Sargysan, S. Data Centers and Indigenous Sovereignty. https://clck.ru/3NNj6F

94 В ООН призывают учитывать права коренных народов при разработке месторождений «критически важных минералов». (2025, 23 апреля). Новости ООН. https://clck.ru/3NNj9a

95 Scandinavian data centres: fewer jobs and less profit than forecast. (2023, April 28). Nordic Labour Journal. https://clck.ru/3NNjBU

96 Andreassen, B. L. (2023, May 30). «Saving the environment» with liquid-cooled data centres. Nordic Labour Journal. https://clck.ru/3NNjEy

97 Tozzi, Ch. (2024, June 13). Why Communities Are Protesting Data Centers. Data Center Knowledge. https://clck.ru/3NNjLR

98 FAQ: Climate change in the Polar regions. SCRIPPS. https://clck.ru/3NNj2m

и изменением землепользования в арктических странах, а именно с неэффективной реализацией прав проживающих там коренных народов (право на землю, право на здоровье и безопасную окружающую среду, право на достойную жизнь, право на сохранение и развитие собственной культуры и др.)[99]. В научной литературе такой подход уже получил название «зеленый империализм», который подразумевает под собой развитие климатических стратегий в интересах мировых элит с дальнейшей маргинализацией уязвимых сообществ, т. е. усилением многовекового неравенства и исторической несправедливости, где ярким примером может служить добыча редкоземельных минералов и металлов для «зеленого сдвига», непропорционально влияющая на территории проживания коренных народов (Boretti, 2025), что в будущем может привести к новым локальным и международным конфликтам – уже сегодня мы наблюдаем территориальные амбиции США по отношению к Гренландии – самоуправляемой автономии в составе Датского королевства, основное население которой составляют инуиты.

Анализ международной правовой базы выявил, что, несмотря на существование большого объема деклараций, конвенций и соглашений, в ней отсутствуют специфичные акты, отвечающие на текущие вызовы новой технологической революции, требующей роста добычи полезных ископаемых, строительства модульных и массивных ЦОД, а также прокладкой глубоководных морских кабелей, для чего все более привлекательными становятся арктические территории, в то время как Антарктика превращается в центр научных исследований климатических изменений, что, как ни парадоксально, связано с ростом вредоносного антропогенного воздействия на регионы этого материка. Учитывая глобальный характер как экологических, так и социальных последствий дальнейшего индустриального и антропогенного освоения территорий арктических стран и Антарктики, а также малую эффективность национальных законодательств в области нивелирования выявленных в данной статье групп рисков, можно заключить, что на сегодняшний день возникла острая необходимость в установлении международного регулирования развития индустрии ЦОД в Арктике и Антарктике, в рамках которого должны быть разработаны единые требования к сертификации и отчетности, а также меры ответственности за нарушения с учетом специфики экологической безопасности этих территорий, их культурных и социальных особенностей.

Список литературы

Ali, S., Poto, M. P., & Murray, E. M. (2024). Arctic Vulnerability: Examining Biosecurity Risks Amidst Climate Change. In G. Panieri, M. P. Poto, & E. M. Murray (Eds.), *Emotional and Ecological Literacy for a More Sustainable Society* (pp. 157–169). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-56772-8_8

Bannan, D., Ólafsdóttir, R., & Hennig, B. D. (2022). Local Perspectives on Climate Change, Its Impact and Adaptation: A Case Study from the Westfjords Region of Iceland. *Climate*, *10*(11), 169. https://doi.org/10.3390/cli10110169

Bargagli, R., & Rota, E. (2024). Environmental contamination and climate change in Antarctic ecosystems: an updated overview. *Environmental Science: Advances*, *3*(4), 543–560. https://doi.org/10.1039/d3va00113j

Boretti, A. (2025). Green imperialism a barrier to equitable progress in the hydrogen economy. *International Journal of Hydrogen Energy*, *105*, 137–147. https://doi.org/10.1016/j.ijhydene.2025.01.195

[99] ООН. (2007, 13 сентября). Декларация ООН о правах коренных народов. https://clck.ru/3NNiz2

Edwards, T. L., Nowicki, S., Marzeion, B. et al. (2021). Projected land ice contributions to twenty-first-century sea level rise. *Nature*, *593*(7857), 74–82. https://doi.org/10.1038/s41586-021-03302-y

Hughes, K. A., Convey, P., & Turner, J. (2021). Developing resilience to climate change impacts in Antarctica: An evaluation of Antarctic Treaty System protected area policy. *Environmental Science & Policy*, *124*, 12–22. https://doi.org/10.1016/j.envsci.2021.05.023

Markkula, I., Turunen, M., Rikkonen, T. et al. (2024). Climate change, cultural continuity and ecological grief: Insights from the Sámi Homeland. *Ambio*, *53*, 1203–1217. https://doi.org/10.1007/s13280-024-02012-9

Mathiot, P., & Jourdain, N. C. (2023). Southern Ocean warming and Antarctic ice shelf melting in conditions plausible by late 23rd century in a high-end scenario. *Ocean Science*, *19*(6), 1595–1615. https://doi.org/10.5194/os-19-1595-2023

Meredith, M. P., Inall, M. E., Brearley, J. A. et al. (2022). Internal tsunamigenesis and ocean mixing driven by glacier calving in Antarctica. *Science Advances*, *8*(47), eadd0720. https://doi.org/10.1126/sciadv.add0720

Orr, J.C., Kwiatkowski, L. & Pörtner, H. O. (2022). Arctic Ocean annual high in PCO2 could shift from winter to summer. *Nature*, *610*, 94–100. https://doi.org/10.1038/s41586-022-05205-y

Parmentier, F. J. W., Thornton, B. F., Silyakova, A., & Christensen, T. R. (2024). Vulnerability of Arctic-Boreal methane emissions to climate change. *Frontiers in Environmental Science*, *12*. https://doi.org/10.3389/fenvs.2024.1460155

Pecuchet, L., Mohamed, B., Hayward, A. et al. (2025). Arctic and Subarctic marine heatwaves and their ecological impacts. *Frontiers in Environmental Science*, *13*. https://doi.org/10.3389/fenvs.2025.1473890

Raimondi, L., Wefing, A.-M., & Casacuberta, N. (2024). Anthropogenic carbon in the Arctic Ocean: Perspectives from different transient tracers. *Journal of Geophysical Research: Oceans*, *129*(1), e2023JC019999. https://doi.org/10.1029/2023JC019999

Rantanen, M., Karpechko, A. Y., Lipponen, A. et al. (2022). The Arctic has warmed nearly four times faster than the globe since 1979. *Commun Earth Environ*, *3*, 168. https://doi.org/10.1038/s43247-022-00498-3

Robinson, S. A. (2022). Climate change and extreme events are changing the biology of Polar Regions. *Global Change Biology*, *28*(20), 5861–5864. https://doi.org/10.1111/gcb.16309

Saunavaara, Ju., & Laine, A. (2021). Research, Development, and Education: Laying Foundations for Arctic and Northern Data Centers. *Arctic and North*, *42*, 145–169. https://doi.org/10.37482/issn2221-2698.2021.42.145

Siegert, M. J., Bentley, M. J., Atkinson, A., Bracegirdle, T. J., Convey, P., Davies, B., Downie, R., Hogg, A. E., Holmes, C., Hughes, K. A., Meredith, M. P., Ross, N., Rumble, J. & Wilkinson, J. (2023). Antarctic extreme events. *Frontiers in Environmental Science*, *11*, 1229283. https://doi.org/10.3389/fenvs.2023.1229283

Suopajärvi, L., Tikkanen, J., Edvardsdóttir, A. Engen, S., Inkilä, E., Iversen, A., … Ólafsdóttir, R. (2024). Geopolitical tensions framing different industries in the European Arctic: aquaculture, forestry, mining, and tourism in question. *Journal of Land Use Science*, *19*(1), 121–133. https://doi.org/10.1080/1747423X.2024.2357576

Taormina, B., Bald, J., Want, A., Thouzeau, G., Lejart, M., Desroy, N., & Carlier, A. (2018). A review of potential impacts of submarine power cables on the marine environment: Knowledge gaps, recommendations and future directions. *Renewable and Sustainable Energy Reviews*, *96*, 380–391. https://doi.org/10.1016/j.rser.2018.07.026

Terhaar, J., Tanhua, T., Stöven, T., Orr, J. C., & Bopp, L. (2020). Evaluation of data-based estimates of anthropogenic carbon in the Arctic Ocean. *Journal of Geophysical Research: Oceans*, *125*(6), e2020JC016124. https://doi.org/10.1029/2020JC016124

Thangam, D., Muniraju, H., Ramesh, R., Narasimhaiah, R., Muddasir Ahamed Khan, N., Booshan, S., Booshan, B., Manickam, T., & Sankar Ganesh, R. (2024). Impact of data centers on power consumption, climate change, and sustainability. In *Computational Intelligence for Green Cloud Computing and Digital Waste Management* (pp. 60–83). IGI Global. https://doi.org/10.4018/979-8-3693-1552-1.ch004

Turunen, M. T., Rikkonen, T., Nikula, A., Tuulentie, S., & Rautio, P. (2024). Between the local and the global? – reindeer herders' perspectives on land use challenges and conflicts in the Sámi homeland, Finland. *Journal of Land Use Science*, *19*(1), 134–149. https://doi.org/10.1080/1747423X.2024.2359606

Yuan, X., Liang, Y., Hu, X., Xu, Y., Chen, Y., & Kosonen, R. (2023). Waste heat recoveries in data centers: A review. *Renewable and Sustainable Energy Reviews*, *188*, 113777. https://doi.org/10.1016/j.rser.2023.113777

Živojinović, I., Elomina, J., Pülzl, H., Calanasan, K., Dabić, I., Ólafsdóttir, R., … Nygaard, V. (2024). Exploring land use conflicts arising from economic activities and their impacts on local communities in the European Arctic. *Journal of Land Use Science*, *19*(1), 186–210. https://doi.org/10.1080/1747423X.2024.2382676

Сведения об авторе

Шумакова Наталья Игоревна – старший преподаватель кафедры конституционного и административного права, Южно-Уральский государственный университет (национальный исследовательский университет)
Адрес: 454080, Россия, г. Челябинск, пр. Ленина, 76
E-mail: shumakovani@susu.ru
ORCID ID: https://orcid.org/0009-0004-6063-0650
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59966654200
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MTE-8168-2025
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

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: 10.87 / Международное право
Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 1 мая 2025 г.
Дата одобрения после рецензирования – 20 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:341.4:004.8
EDN: https://elibrary.ru/gcvuaw
DOI: https://doi.org/10.21202/jdtl.2025.15

International Fundamentals of Legal Regulation of the Data Center Industry in the Arctic States and the Antarctic

Nataliya Igorevna Shumakova
South-Ural State University (National Research University), Chelyabinsk, Russia

Keywords

data processing centers,
digital technologies,
environmental law,
environmental security,
indigenous peoples,
international law,
law of indigenous peoples,
law,
the Antarctic,
the Arctic

Abstract

Objective: to critically assess the effectiveness of existing international legal norms under the new challenges of technological progress, related to the development of the data center industry in the Arctic states and the Antarctic.

Methods: the methodological basis of the research is a set of special and general methods of scientific cognition, including methods of comparative law, content analysis, deduction, induction, formal logical method and document analysis. The author turns to interdisciplinary approaches in order to objectively assess the environmental, social and legal risks arising from the data center industry growth in regions with increased climatic and social vulnerability.

Results: the article analyzed international legal acts regulating the functioning of data centers in polar regions. It identified the key risks and divided them into environmental (instability of local ecosystems, lack of adaptability to rapid changes, risk of losing biological diversity, and greenhouse gas emissions) and social (marginalization and violation of the rights of indigenous peoples, loss of traditional cultures and lifestyles, increased social tension). The author points out that new conflicts and challenges will inevitably emerge due to the insufficient effectiveness of national and international regulatory mechanisms. The states the need to create specialized international legal instruments taking into account the specifics of the environmental safety of the polar territories.

Scientific novelty: for the first time, the article provides a comprehensive analysis of the integral risks and drawbacks of the current international legislation on data center industry in the Arctic states and the Antarctic. The author provides a comparative analysis of the normative framework and shows the inconsistency between the "soft law" principles application on the polar regions and the fourth technological revolution. The author substantiates the requirement to create new certification and reporting procedures throughout the lifecycle of data centers, taking into account the legal and cultural context.

Practical significance: the results are focused on improving international and national policies in the sphere of regulating the data center industry and on developing certification and reporting standards that could be effective in the climatic, social and economic conditions of the Arctic states and the Antarctic. The research is aimed at minimizing the negative impact of anthropogenic factors and ensuring a balance between industrial development and the preservation of unique natural and cultural landscapes.

For citation

Shumakova, N. I. (2025). International Fundamentals of Legal Regulation of the Data Center Industry in the Arctic States and the Antarctic. *Journal of Digital Technologies and Law, 3*(3), 369–396. https://doi.org/10.21202/jdtl.2025.15

References

Ali, S., Poto, M. P., & Murray, E. M. (2024). Arctic Vulnerability: Examining Biosecurity Risks Amidst Climate Change. In G. Panieri, M. P. Poto, E. M. Murray (Eds.), *Emotional and Ecological Literacy for a More Sustainable Society* (pp. 157–169). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-56772-8_8

Bannan, D., Ólafsdóttir, R., & Hennig, B. D. (2022). Local Perspectives on Climate Change, Its Impact and Adaptation: A Case Study from the Westfjords Region of Iceland. *Climate*, *10*(11), 169. https://doi.org/10.3390/cli10110169

Bargagli, R., & Rota, E. (2024). Environmental contamination and climate change in Antarctic ecosystems: an updated overview. *Environmental Science: Advances*, *3*(4), 543–560. https://doi.org/10.1039/d3va00113j

Boretti, A. (2025). Green imperialism a barrier to equitable progress in the hydrogen economy. *International Journal of Hydrogen Energy*, *105*, 137–147. https://doi.org/10.1016/j.ijhydene.2025.01.195

Edwards, T. L., Nowicki, S., Marzeion, B. et al. (2021). Projected land ice contributions to twenty-first-century sea level rise. *Nature*, *593*(7857), 74–82. https://doi.org/10.1038/s41586-021-03302-y

Hughes, K. A., Convey, P., & Turner, J. (2021). Developing resilience to climate change impacts in Antarctica: An evaluation of Antarctic Treaty System protected area policy. *Environmental Science & Policy*, *124*, 12–22. https://doi.org/10.1016/j.envsci.2021.05.023

Markkula, I., Turunen, M., Rikkonen, T. et al. (2024). Climate change, cultural continuity and ecological grief: Insights from the Sámi Homeland. *Ambio*, *53*, 1203–1217. https://doi.org/10.1007/s13280-024-02012-9

Mathiot, P., & Jourdain, N. C. (2023). Southern Ocean warming and Antarctic ice shelf melting in conditions plausible by late 23rd century in a high-end scenario. *Ocean Science*, *19*(6), 1595–1615. https://doi.org/10.5194/os-19-1595-2023

Meredith, M. P., Inall, M. E., Brearley, J. A. et al. (2022). Internal tsunamigenesis and ocean mixing driven by glacier calving in Antarctica. *Science Advances*, *8*(47), eadd0720. https://doi.org/10.1126/sciadv.add0720

Orr, J.C., Kwiatkowski, L. & Pörtner, H. O. (2022). Arctic Ocean annual high in PCO2 could shift from winter to summer. *Nature*, *610*, 94–100. https://doi.org/10.1038/s41586-022-05205-y

Parmentier, F. J. W., Thornton, B. F., Silyakova, A., & Christensen, T. R. (2024). Vulnerability of Arctic-Boreal methane emissions to climate change. *Frontiers in Environmental Science*, *12*. https://doi.org/10.3389/fenvs.2024.1460155

Pecuchet, L., Mohamed, B., Hayward, A. et al. (2025). Arctic and Subarctic marine heatwaves and their ecological impacts. *Frontiers in Environmental Science*, *13*. https://doi.org/10.3389/fenvs.2025.1473890

Raimondi, L., Wefing, A.-M., & Casacuberta, N. (2024). Anthropogenic carbon in the Arctic Ocean: Perspectives from different transient tracers. *Journal of Geophysical Research: Oceans*, *129*(1), e2023JC019999. https://doi.org/10.1029/2023JC019999

Rantanen, M., Karpechko, A. Y., Lipponen, A. et al. (2022). The Arctic has warmed nearly four times faster than the globe since 1979. *Commun Earth Environ*, *3*, 168. https://doi.org/10.1038/s43247-022-00498-3

Robinson, S. A. (2022). Climate change and extreme events are changing the biology of Polar Regions. *Global Change Biology*, *28*(20), 5861–5864. https://doi.org/10.1111/gcb.16309

Saunavaara, Ju., & Laine, A. (2021). Research, Development, and Education: Laying Foundations for Arctic and Northern Data Centers. *Arctic and North*, *42*, 145–169. https://doi.org/10.37482/issn2221-2698.2021.42.145

Siegert, M. J., Bentley, M. J., Atkinson, A., Bracegirdle, T. J., Convey, P., Davies, B., Downie, R., Hogg, A. E., Holmes, C., Hughes, K. A., Meredith, M. P., Ross, N., Rumble, J. & Wilkinson, J. (2023). Antarctic extreme events. *Frontiers in Environmental Science*, *11*, 1229283. https://doi.org/10.3389/fenvs.2023.1229283

Suopajärvi, L., Tikkanen, J., Edvardsdóttir, A. Engen, S., Inkilä, E., Iversen, A., … Ólafsdóttir, R. (2024). Geopolitical tensions framing different industries in the European Arctic: aquaculture, forestry, mining, and tourism in question. *Journal of Land Use Science*, *19*(1), 121–133. https://doi.org/10.1080/1747423X.2024.2357576

Taormina, B., Bald, J., Want, A., Thouzeau, G., Lejart, M., Desroy, N., & Carlier, A. (2018). A review of potential impacts of submarine power cables on the marine environment: Knowledge gaps, recommendations and future directions. *Renewable and Sustainable Energy Reviews*, *96*, 380–391. https://doi.org/10.1016/j.rser.2018.07.026

Terhaar, J., Tanhua, T., Stöven, T., Orr, J. C., & Bopp, L. (2020). Evaluation of data-based estimates of anthropogenic carbon in the Arctic Ocean. *Journal of Geophysical Research: Oceans*, *125*(6), e2020JC016124. https://doi.org/10.1029/2020JC016124

Thangam, D., Muniraju, H., Ramesh, R., Narasimhaiah, R., Muddasir Ahamed Khan, N., Booshan, S., Booshan, B., Manickam, T., & Sankar Ganesh, R. (2024). Impact of data centers on power consumption, climate change, and sustainability. In *Computational Intelligence for Green Cloud Computing and Digital Waste Management* (pp. 60–83). IGI Global. https://doi.org/10.4018/979-8-3693-1552-1.ch004

Turunen, M. T., Rikkonen, T., Nikula, A., Tuulentie, S., & Rautio, P. (2024). Between the local and the global? – reindeer herders' perspectives on land use challenges and conflicts in the Sámi homeland, Finland. *Journal of Land Use Science*, *19*(1), 134–149. https://doi.org/10.1080/1747423X.2024.2359606

Yuan, X., Liang, Y., Hu, X., Xu, Y., Chen, Y., & Kosonen, R. (2023). Waste heat recoveries in data centers: A review. *Renewable and Sustainable Energy Reviews*, *188*, 113777. https://doi.org/10.1016/j.rser.2023.113777

Živojinović, I., Elomina, J., Pülzl, H., Calanasan, K., Dabić, I., Ólafsdóttir, R., … Nygaard, V. (2024). Exploring land use conflicts arising from economic activities and their impacts on local communities in the European Arctic. *Journal of Land Use Science*, *19*(1), 186–210. https://doi.org/10.1080/1747423X.2024.2382676

Author information

Nataliya I. Shumakova – Senior Lecturer, Department of Constitutional and Administrative Law, South-Ural State University (National Research University)
Address: 76 Lenin prospekt, 454080, Chelyabinsk, Russia
E-mail: shumakovani@susu.ru
ORCID ID: https://orcid.org/0009-0004-6063-0650
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=59966654200
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MTE-8168-2025
РИНЦ Author ID: https://www.elibrary.ru/author_items.asp?authorid=1211522

Conflict of interest

The author declares no conflict of interests.

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 1, 2025
Date of approval – May 20, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/smgmxq
DOI: https://doi.org/10.21202/jdtl.2025.16

Нейрохакинг в эпоху цифровизации и искусственного интеллекта: правовые аспекты защиты нейронной информации

Диого Перейра Коэльо

Севильский университет, Севилья, Испания

Ключевые слова

интерфейс «мозг – компьютер»,
искусственный интеллект,
киберпреступность,
метавселенная,
нейробезопасность,
нейропреступность,
нейротехнологии,
нейрохакинг,
право,
цифровые технологии

Аннотация

Цель: внесение вклада в осмысление концепции нейропреступности, а также в изучение текущих и будущих рисков с точки зрения нейробезопасности в условиях развития цифровизации и искусственного интеллекта.

Методы: в исследовании применен критико-описательный анализ связи между киберпреступностью и нейропреступностью, проведено концептуальное разграничение интерфейса «мозг – компьютер» и вариантов его использования, выполнено описание различий между нейронными и психическими манипуляциями. Исследуется правовая автономия преступлений против психической неприкосновенности по отношению к преступлениям против физической неприкосновенности. Методологический аппарат включает анализ существующих прототипов нейропреступлений на основе четырехфазного цикла интерфейса «мозг – компьютер» и изучение специфики нейрохакинга в контексте метавселенной и технологий искусственного интеллекта.

Результаты: исследование выявило сущностные характеристики нейрохакинга как неправомерного использования нейронных устройств для получения несанкционированного доступа к нейронной информации и ее манипулирования. Определены четыре основных типа приложений интерфейса «мозг – компьютер», подверженных нейрохакингу: нейромедицинские приложения, системы аутентификации пользователей, видеоигры и приложения на базе смартфонов. Установлены модальности нейрохакинга на каждой фазе цикла интерфейса «мозг – компьютер»: манипуляции на этапе ввода нейронной информации, измерения и записи мозговой активности, декодирования и классификации нейронной информации, а также на этапе вывода результата. Проанализированы специфические угрозы нейрохакинга в эпоху цифровизации, включая иммерсивные атаки и атаки типа «человек – джойстик» в метавселенной.

Научная новизна: впервые проведено комплексное разграничение концепций нейропреступности и киберпреступности с выделением их специфических правовых последствий. Предложена авторская классификация нейропреступлений на основе четырехфазного цикла интерфейса «мозг – компьютер». Обоснована необходимость выделения психической неприкосновенности как самостоятельного объекта правовой защиты, отличного от защиты физической неприкосновенности. Впервые исследованы особенности нейрохакинга в контексте метавселенной и технологий искусственного интеллекта, включая анализ новых типов атак и угроз нейробезопасности.

Практическая значимость: результаты исследования имеют важное значение для развития правового регулирования в области нейробезопасности и разработки соответствующих нормативных актов. Выявленные типы нейропреступлений и их классификация могут служить основой для создания специализированного законодательства о защите нейронных данных и психической неприкосновенности. Практические рекомендации по обеспечению нейробезопасности интерфейсов «мозг – компьютер» востребованы в медицинской практике, индустрии видеоигр, системах аутентификации и разработке приложений для смартфонов.

Для цитирования

Коэльо, Д. П. (2025). Нейрохакинг в эпоху цифровизации и искусственного интеллекта: правовые аспекты защиты нейронной информации. *Journal of Digital Technologies and Law*, *3*(3), 397–430. https://doi.org/10.21202/jdtl.2025.16

Содержание

Введение

Есть мнение, что незаконный доступ к нейронной информации или манипулирование ею невозможны и никогда не будут осуществимы в том виде, в котором это часто предполагается и которого опасаются[1]. Основной причиной этого является ограниченное понимание нейронного кода, т. е. языка, с помощью которого мозг кодирует и обрабатывает информацию. Чтобы это стало возможным, потребовалось бы расшифровать нейронный код для достижения конкретного результата (доступа или манипуляции) и среди миллиардов нейронов, существующих в человеческом мозге, определить, какой именно из них следует стимулировать[2]. В настоящее время ученые только представляют, какую область мозга стимулировать, однако определение конкретного нейрона по-прежнему остается недостижимой задачей. Кроме того, у разных субъектов за определенную функцию могут отвечать разные нейроны[3]. С другой стороны, есть мнение, что невозможно повлиять на поведение субъекта, стимулируя только один нейрон, поскольку функция мозга зависит от скоординированной активности сложных нейронных цепей, включающих сотни или миллиарды нейронов. Скоординированная стимуляция больших сетей нейронов с целью навязывания целенаправленного и специфического

1 Fields, R. D. (2022). Hacking the brain: More fantasy than reality. The UNESCO Courier. Should we be afraid of neuroscience? (p. 9). UNESCO. https://clck.ru/3Nkhbr

2 Там же.

3 Там же.

поведения в целях манипулирования и ментального контроля представляется практически невозможной[4].

В целом все может считаться системой, включая человеческий мозг. И, как и все системы, человеческий мозг также может являться объектом «взлома». Есть мнение[5], что человечество «взломало» законы природы[6]. Подсчет карт в блэкджеке – это взлом[7]. В большинстве видов спорта люди прибегают к «взлому». Так, в «Формуле-1» команды пытаются найти новые способы изменения дизайна автомобилей, которые прямо не запрещены регламентом[8]. Предвыборные махинации являются хакерством в политике[9]. Кроме того, в финансовом и деловом мире также используются различные методы взлома. Большинство игроков на рынке, от предпринимателей до финансовых учреждений, пытаются найти лазейки в системе (т. е. в законе) в основном для того, чтобы получить преимущество перед конкурентами. В частности, они используют ситуации, которые прямо не запрещены, но представляют собой намеренный (или нет) подрыв системы. Например, компании Uber[10] и Airbnb[11], как и другие крупные технологические корпорации (организации), всегда нарушали правила, установленные правовыми системами ряда юрисдикций. Таким образом, концепция «воспрепятствования», вероятно, так же стара, как и понятия «пробел в законе» или «пробел в системе», и так же стара, как сама человеческая цивилизация, поскольку и человека, видимо, можно взломать. В этом контексте человеческий мозг представляет собой систему, которая, появившись как средство выживания и, прежде всего, размножения, подвергалась оптимизации в результате непрерывного взаимодействия с окружающей средой на протяжении миллионов лет.

---

4 Там же.

5 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4

6 Английское слово hacker обычно переводится на другие языки как «компьютерный пират». Однако использование такого перевода слова представляется неточным. Хакер может действовать как «пират», а «пират» может действовать как «хакер», но эти два определения, по-видимому, не эквивалентны. Скорее, они просто дополняют друг друга. Хакеры используют системы, будь то на компьютере, в телефоне, при личном общении или в любом другом аспекте человеческой жизни. Как правило, они действуют законными способами. Хакеры (или «взломщики») незаконно пытаются расшифровать (взломать) систему ради развлечения либо для получения определенного результата или преимущества. Несмотря на проблемы с семантикой и терминологическую путаницу, в данной статье в основном будет использоваться термин «хакер», потому что он наиболее известен, а также для легкости чтения. См. Ribeiro, J. B. (2019, 12 Fevereiro). 'Hacker' vs 'Pirata Informático': a riqueza de uma definição perdida na tradução. SH/FTER. https://clck.ru/3NkhkJ

7 Keating, S. (2022). How a magician-mathematician revealed a casino loophole. BBC. https://clck.ru/3Nkhnx

8 Straw, E. (2022, February 22). F1's new philosophy in combatting design loopholes. The Race. https://clck.ru/3Nkhq9

9 Ax, J. (2023). North Carolina court allows partisan gerrymandering. Reuters. https://clck.ru/3Nkhrs

10 Henley, J. (2017, September 29). Uber clashes with regulators in cities around the world. The Guardian. https://clck.ru/3Nkht2

11 Neubauer, I. L. (2019, August 30). Countries that are cracking down on Airbnb. The New Daily. https://goo.su/UcOHh

Таким образом, когнитивный хакинг, по-видимому, является мощным инструментом[12] в отношениях между людьми, и одной из его разновидностей является техника манипулирования, известная как «социальная инженерия». В области киберпреступности единственное новшество заключается в использовании технологий для взлома, потому что компьютеры, как и человеческий мозг, также являются системами. За последние несколько десятилетий мы стали свидетелями того, как методы взлома адаптировались к компьютеризации традиционных систем. Эта компьютеризация, по-видимому, изменила методы взлома в трех аспектах: масштаб, охват и скорость. Во-первых, она усилила и расширила характер взломов, тем самым увеличив их масштабы. Во-вторых, растущее число разработок программного и аппаратного обеспечения позволило системам развиваться быстрее, чем предполагалось изначально. Скорость работы компьютеров не отставала от этого развития, что также способствовало использованию методов взлома[13]. С переходом от Web 1.0 к Web 2.0 и Web 3.0, а в последнее время и к Web 4.0 появились новые прорывные технологии[14], и использование цифровых или искусственных компьютерных систем расширяется все более быстрыми темпами (Ienca & Haselager, 2016)[15]. В конечном счете с развитием киберпреступности методы взлома сосредоточатся на человеческом

12 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4. Например, многие из влиятельных социальных систем, составляющих основу общества, такие как демократия и рыночная экономика, зависят от решений, принимаемых людьми. Этот процесс может стать объектом когнитивного взлома, например, через социальные коммуникации. Современная реклама, персонализированная в соответствии с нашими предпочтениями и поведением, представляет собой своего рода массовый взлом человеческого мозга, в частности сознательных психических процессов, включая предшествующее бессознательное состояние. То же относится к дезинформации (часто распространяемой самими СМИ), которая разрушает общепринятое представление о реальности. Постоянное использование таких терминов, как «терроризм» или «кибертерроризм», в средствах массовой информации и в выступлениях политиков также представляет собой взлом когнитивной системы с целью убедить людей в том, что это более серьезная угроза, чем она есть на самом деле, и тем самым вызвать страх и исказить оценку риска.

13 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkhe4

14 Термин «прорывные технологии» появился относительно недавно. Он подразумевает изменение стандартов, моделей или технологий, уже существующих на рынке. Другими словами, технологическая инновация, продукт или услуга с так называемыми прорывными характеристиками отличаются разнообразием, революционностью, новаторством, они никогда не рассматривались и не применялись в данном контексте. См. Dufloth, R. (2017). Novas tecnologias e o futuro do profissional do Direito. Mgalhas. https://clck.ru/3Nm3jy

15 В целом технологии, связанные с Web 1.0, Web 2.0, Web 3.0 и Web 4.0, позволяют пользователям напрямую взаимодействовать с данными и системами и могут использоваться для решения широкого спектра повседневных и профессиональных задач. Например, системы GPS помогают в геолокации и пространственной навигации, портативные устройства отслеживают такие процессы организма, как частота сердечных сокращений, потребление калорий и снижение веса. Также в качестве примера можно привести персональные компьютеры, которые помогают в решении когнитивных задач, таких как арифметические вычисления, создание письменных текстов и запоминание информации. Цифровые активы на основе блокчейна позволяют осуществлять международные транзакции в считаные минуты или даже секунды, а системы искусственного интеллекта позволяют мгновенно создавать оригинальные тексты, изображения или видеоролики. См. Nath, K. (2022). Evolution of the Internet Web 1.0 to Metaverse: The Good, the Bad and the Ugly. Research Gate. https://clck.ru/3NkiAo

мозге и психике как таковой, в частности, в форме «нейропреступлений» и «нейрохакинга» (также обычно называемого взломом мозга). При таком сценарии увеличение масштабов, сферы применения и скорости методов взлома будет становиться все более заметным.

Цель работы – внести вклад в изучение и первоначальное формулирование предмета, понимание которого никогда не будет достаточным не в последнюю очередь из-за высокого уровня юридических активов, о которых идет речь.

1. От киберпреступности к нейропреступности

1.1. Связь между киберпреступностью и нейропреступностью

Общепринятого определения киберпреступности не существует. Термины «киберпреступность», «компьютерная преступность», «преступления, связанные с использованием компьютеров» или «преступления, связанные с использованием высоких технологий» используются часто, но достаточно произвольно. На международном, общеевропейском или национальном уровне нет единого мнения относительно формулировок, определений, типологии или классификации киберпреступности (Rodrigues, 2009; Vasconcelos Casimiro, 2000). Четкого определения понятий «киберпреступность» или «компьютерное преступление» нет и в португальском законодательстве[16]. В литературе и юриспруденции также нет единообразной концепции (Venâncio, 2011). Отсутствие единообразия проявляется в том, что термин «киберпреступность» в общем и абстрактном виде охватывает целый ряд преступлений, совершаемых с использованием информационно-коммуникационных технологий. Этот термин включает как классические преступные деяния, так и новые виды преступлений.

По мнению Европейской комиссии, киберпреступления – это «преступные действия, совершаемые с использованием сетей электронных коммуникаций и информационных систем или против таких сетей и систем»[17]. Такие преступления делятся на три вида. Во-первых, это традиционные формы преступной деятельности, но использующие Интернет (включая кражу идентичности и фишинг) для совершения преступлений (например, компьютерное мошенничество или спуфинг). К этим традиционным формам также относится международная электронная торговля наркотиками, оружием и видами животных, находящимися под угрозой исчезновения. Во-вторых, к киберпреступлениям относится публикация в Интернете незаконного контента, такого как материалы, подстрекающие к терроризму, насилию, расизму и ксенофобии или сексуальному насилию над несовершеннолетними. И, наконец, это преступления, совершаемые исключительно в электронных сетях; они представляют собой новые и часто крупномасштабные деяния, которые были «неизвестны в эпоху

[16] Например, в Португалии в дополнение к видам преступлений, предусмотренным Законом № 109/2009 от 15 сентября, который развивает положения национального законодательства о киберпреступности (https://clck.ru/3Nkxa7), другие виды преступлений подобного рода предусмотрены в Уголовном кодексе Португалии и в различных других отдельных правовых источниках.

[17] European Commission. (2007). Towards a general policy on the fight against cyber crime. Communication from the Commission to the European Parliament, the Council and the Committee of the Regions. https://clck.ru/3NkiNh

до Интернета». В последнем случае преступные агенты атакуют системы или целые информационные инфраструктуры и даже конфиденциальную государственную информацию (что представляет собой национальную угрозу). При этом, по данным Европейской комиссии, эти атаки могут осуществляться через «ботнеты» (сеть роботов), т. е. преступные агенты распространяют вредоносное программное обеспечение (ПО), которое превращает компьютер пользователя в бота. Зараженная сеть или информационная инфраструктура используются для совершения преступлений без ведома их пользователей. Итак, компьютерное преступление представляет собой любое деяние, в ходе которого компьютер или аналогичная технология либо служит средством достижения преступной цели, либо представляет собой лишь символическую цель этого деяния или даже объект преступления (Marques & Martins, 2006). Поэтому необходимо проводить различие между «компьютерным преступлением», при котором объектом преступления являются информационные технологии, и «преступлением, совершенным с использованием компьютерных средств», когда информационные технологии являются средством совершения преступления.

По этой логике, если преступление совершается с использованием нейронных интерфейсов и, помимо того, что представляет физическую угрозу для пользователей, также оказывает глубокое влияние на их поведение и самовосприятие, мы имеем дело с «нейропреступлением»[18]. Особую актуальность приобретает неправомерное использование информационных технологий в контексте нейротехнологий, поскольку они применяются (прямо или косвенно) к работе мозга, одного из самых важных органов человека. Человеческий мозг не только вносит значительный вклад в жизненные процессы, такие как размножение и поддержание жизни, но и обеспечивает сознание, восприятие, способность мыслить и рассуждать, память и речь. Кроме того, он по-прежнему имеет огромное значение для поведения человека и его самовосприятия как существа или индивидуума, наделенного чувствами и эмоциями (Ienca & Haselager, 2016). Таким образом, нейропреступление можно определить как любое деяние, в котором человеческий мозг и/или психика служит средством достижения преступной цели либо является символической целью этого деяния или объектом преступления. Следовательно, необходимо проводить различие между «нейропреступлением», при котором мозг и/или психика прямо или косвенно являются объектом преступления, и «преступлением, совершенным с использованием нейронных и/или психических манипуляций», при котором мозг и/или психика являются средством совершения преступления. Таким образом, как мы увидим в п. 3 этого раздела, необходимо также проводить различие между нейронными манипуляциями и чисто психическими манипуляциями. Кроме того, при нейропреступлении может совершаться не прямой, а лишь косвенный доступ к мозгу или сохраненной информации. Например, функции нейронного устройства могут быть ограничены, модифицированы или разрегулированы. С учетом современных достижений в области технологий нейронной инженерии (в основном реализуемых в секторе здравоохранения) этот сценарий становится все более реальным. В этом случае преступник воздействует на мозг жертвы косвенно, поскольку во время атаки не осуществляется прямой доступ к нейронной системе и значительные манипуляции с ней не производятся. Тем не

[18] Данный термин обычно относится к преступной деятельности, совершаемой с использованием нейронных устройств.

менее психическое состояние жертвы подвергается существенному влиянию, например, поведение ограничивается или сковывается, наступает эмоциональная реакция в виде паники, страха или психологических расстройств, возникают травмирующие воспоминания. Стоит отметить, что при определенных обстоятельствах исполнитель и объект преступления меняются ролями. Например, пользователи с психической нестабильностью могут повредить свои нейронные устройства, чтобы совершить попытку самоубийства (Ienca & Haselager, 2016). Таким образом, в широком смысле понятие нейропреступления можно определить как преступление против разума человека или группы людей, совершаемое с использованием нейронных и/или чисто психических манипуляций с помощью нейронного устройства и с намерением прямо или косвенно причинить физический или психический вред, включая ущерб репутации и/или имуществу.

В области нейропреступности и нейронной стимуляции в настоящее время считаются особенно важными два типа нейронных устройств. Во-первых, это стимуляторы мозговой активности, особенно системы глубокой стимуляции мозга (deep brain stimulation, DBS) и транскраниальной стимуляции постоянным током (transcranial direct current stimulation, tDCS). Во-вторых, это интерфейсы «мозг – компьютер» (brain-computer interface, BCI). Оба типа устройств обеспечивают прямой доступ к нейронным вычислениям, хотя и разными способами (моделирование мозга или считывание активности мозга). Кроме того, они доступны не только как медицинские технологии, но и как продукты, предназначенные для условно здоровых пользователей. Поэтому эти устройства вызывают многочисленные вопросы с точки зрения «нейробезопасности». Фактически на сегодняшний день основными нейронными устройствами, используемыми для взлома (даже при наличии экспериментальных данных и в контексте реальных ситуаций), являются интерфейсы «мозг – компьютер», поэтому мы рассмотрим только эти устройства (Ienca & Haselager, 2016).

1.2. Концепция интерфейса «мозг – компьютер» и примеры его использования

В отличие от простых нейростимуляторов (электронных устройств, подобных кардиостимуляторам) интерфейсы «мозг – компьютер» (далее – ИМК) используются не для стимуляции мозга, а для установления прямого канала связи, который, минуя периферическую нервную систему и мышцы, позволяет пользователям управлять внешним компьютером исключительно посредством мозговой активности (Ienca & Haselager, 2016; Vallabhaneni et al., 2005). Они впервые появились в области клинической медицины как терапевтическая технология для оказания медицинской помощи неврологическим пациентам. В клиническом контексте приложения ИМК используются для восстановления, поддержания и усиления двигательных, когнитивных или сенсорных функций у пациентов, страдающих неврологическими расстройствами, которые непосредственно влияют на развитие моторики и/или когнитивные и сенсорные функции, включая травмы спинного мозга, инсульты и неврологические двигательные заболевания, такие как боковой амиотрофический склероз (БАС) и мышечная дистрофия (Ienca & Haselager, 2016).

ИМК делятся на два типа: инвазивные и неинвазивные. Инвазивные ИМК требуют хирургической имплантации электродных решеток в центральную нервную систему или простого прямого подключения. Неинвазивные ИМК регистрируют

мозговую активность с помощью электродов, расположенных снаружи черепа, т. е. с помощью технологий нейровизуализации, таких как электроэнцефалография (далее – ЭЭГ) и электромиография. В обоих случаях устанавливается прямое взаимодействие между мозгом пользователя и нейронным устройством. Как правило, это взаимодействие представляет собой четырехфазный цикл (Ienca & Haselager, 2016; Van Gerven et al., 2009; Bernal et al., 2022)[19]. Первая фаза состоит из ввода нейронной информации (т. е. создания определенной мозговой активности) пользователем в ответ на заданный стимул (всякий раз, когда пользователь ИМК хочет выполнить определенную умственную задачу или достичь определенного когнитивного состояния). Вторая фаза включает измерения и регистрацию мозговой активности. На этом этапе интерфейс обнаруживает, измеряет и записывает паттерны мозговой активности пользователя во время когнитивного процесса или выполнения определенной умственной задачи. На третьем этапе необработанные нейронные данные (нейронная информация), полученные в результате второго этапа, декодируются, чтобы оценить их основные характеристики и классифицировать. После декодирования и классификации данные преобразуются в определенные выходные данные, необходимые пользователю. В целом результатом четвертого этапа является выполнение действий, изначально запланированных, желаемых или считающихся полезными для пользователя, посредством управления приложениями, подключенными к ИМК. Управляемые приложения представляют собой устройства с электроприводом, такие как электрические инвалидные кресла или роботизированные протезы конечностей, сенсорные устройства и другие типы программных и аппаратных приложений (включая мобильные приложения и сотовые телефоны). По завершении каждого из этапов пользователь может увидеть достигнутый результат и приступить к следующему этапу (Ienca & Haselager, 2016). Примером применения этих технологий является Герт Ян Оскам, который после аварии на мотоцикле более десяти лет страдал параличом нижних конечностей, но теперь снова может ходить с помощью ИМК (хотя пока и не вполне свободно)[20].

Сегодня приложения ИМК доступны не только в клинических условиях, но и для широких слоев населения (Mochan et al., 2025). На рынке появилось множество коммерческих приложений для ИМК-устройств на основе ЭЭГ, которые становятся все более популярными как в сфере видеоигр, так и для повседневной деятельности (Ienca & Haselager, 2016)[21]. ИМК используются также в индустрии электронных телекоммуникаций. Так, некоторые мобильные приложения (например, приложение Xwave, выпущенное более 10 лет назад!) позволяют устанавливать прямое соединение с совместимыми мобильными телефонами iPhone через определенные

[19] В этой связи следует отметить, что ИМК могут быть классифицированы в зависимости от степени их инвазивности. В неинвазивных системах электроды размещаются на коже головы, тогда как инвазивные системы требуют хирургической процедуры для размещения электродов внутри черепа – либо на поверхности головного мозга, либо даже внутри самого мозга.

[20] Whang, O. (2023). Brain Implants Allow Paralyzed Man to Walk Using His Thoughts. https://clck.ru/3Nkxhk

[21] Например, см. веб-сайты компаний Emotiv Inc. и Neurosky Inc., которые являются пионерами в области коммерциализации неинвазивных, интуитивно понятных и доступных ИМК для видеоигр, интерактивного телевидения и систем управления: https://clck.ru/3NkiYN и https://clck.ru/3NkiZy См. также Gordon, L. (2020, December 16). Brain-controlled gaming exists, though ethical questions loom over the tech. The Washington Post. https://clck.ru/3Nkicf

типы наушников и записывать мозговые волны (Ienca & Haselager, 2016)[22]. Сектор вооружений в настоящее время также разрабатывает несколько приложений ИМК (Ienca & Haselager, 2016; Czech, 2021). Например, Агентство перспективных исследовательских проектов Министерства обороны США (DARPA) финансирует широкий спектр проектов в области ИМК, в основном направленных на восстановление поведенческих или нейронных функций у солдат, а также на улучшение подготовки и результативности военнослужащих и агентов секретных служб (Ienca & Haselager, 2016; Kotchetkov et al., 2010; Miranda et al., 2015). Основываясь на огромном потенциале управления мозгом с помощью нейронных вычислительных устройств и учитывая возможные преимущества и базовую функциональность, можно прогнозировать, что ИМК постепенно заменит клавиатуру, сенсорный экран, компьютерную мышь и даже технологию голосовой поддержки, поскольку потребители смогут взаимодействовать непосредственно с компьютерами (Ienca & Haselager, 2016; Yuan et al., 2010; Radu, 2024). Однако, как мы покажем ниже, хотя потенциальные выгоды от ожидаемой массовой коммерциализации определенных клинических и неклинических применений технологии ИМК представляются значительными и хорошо изученными, остаются в значительной степени не изученными очень серьезные (и, возможно, непоправимые) риски, связанные с нейробезопасностью. Чтобы понять эти риски, необходимо сначала провести различие между нейронными и чисто психическими манипуляциями.

1.3. Различия между нейронными и психическими манипуляциями

После более чем 2000 лет философских споров и самых последних впечатляющих научных достижений в области искусственного интеллекта (далее – ИИ) и обработки данных проблема дуализма сознания и мозга сохраняется и по-прежнему не поддается однозначному решению (Bublitz & Merkel, 2014; Moulin, 2022). По словам Maria Fernanda Palma, абсолютное отрицание дуализма сознания и мозга или сведение феноменов сознания к состояниям мозга может оказать значительное влияние на реальные поведенческие основания юридической ответственности; особенно это касается добровольных действий или истинной способности отдельных лиц считаться виновными по уголовному закону[23]. Если акт сознания не предшествует принятию решения, то неизбежно ставится под сомнение такой критерий возникновения или усиления ответственности за намеренное деяние, как свободное и осознанное решение. В этом смысле абсолютное самоопределение человека как источника ответственности ставится под сомнение, если предположить, что разумное решение может быть вычислено подобно алгоритму и имитировано с помощью математических процессов. Нейробиология, по-видимому, предлагает натуралистическую редукцию разума и состояний сознания, тогда как наука о данных и искусственном интеллекте рассматривает функционирование мозга как автономный биологический процесс, в котором могут воспроизводиться психические состояния и их связь с поведением человека. Эта точка зрения неожиданно приводит к переосмыслению дуалистической

22 PLX Devices Inc. XWave – Mind Interface Introduction and Teaser. 2010. https://clck.ru/3NkifC

23 Fernanda Palma, M. (2021–2022). Ciberneurodireito. Powerpoint Presentation. Short Course in Criminal Law on Artificial Intelligence and Artificial Intelligence in Criminal Law. FDUL. IDPCC/ CIDPCC, 4.

гипотезы, рассматривающей мозг всего лишь как одну из возможных основ человеческого поведения. Право как таковое, а также в его связях со смежными науками направлено на изучение того, имеет ли конкретное психическое состояние причинно-следственную связь с работой мозга и обязательно ли оно подразумевает определенное поведение, а также в какой степени оно поддается контролю[24].

По мнению Jan Christoph Bublitz и Reinhard Merkel, все психические явления так или иначе связаны с деятельностью мозга. Это дает основания утверждать, что законодателю следует проявлять осторожность при описании отношений между сознанием и мозгом как дуалистических; не в последнюю очередь причина этого в том, что трудно идентифицировать изменения в психическом состоянии, не выявив также определенных изменений на церебральном (нейронном) уровне. Также утверждают, что психические состояния не только коррелируют с определенным состоянием мозга, но и вызываются или осознаются на основе определенного физического состояния. Однако всякий раз, когда рассматривается более точное и конкретное описание этой корреляции, возникает множество проблем, поскольку нет единого мнения относительно связи с причинами или процессом «осознания» (Bublitz & Merkel, 2014). Таким образом, несмотря на существующую в настоящее время в психиатрии тенденцию классифицировать любое психическое расстройство как расстройство головного мозга в строгом смысле этого слова, некоторые ученые утверждают, что психические травмы не обязательно связаны с физическими нарушениями. В принципе, это не мозг «решает», «страдает» или ощущает «моральный ущерб». Напротив, все указывает на то, что мы имеем дело с психическими состояниями/процессами людей, а не с качествами физических объектов. Для нормативных целей, связанных с понятиями «вред» или «расстройство/дисфункция», можно считать доказанным, что психика и мозг заслуживают индивидуального внимания (Bublitz & Merkel, 2014). Например, психические расстройства/дисфункции, по-видимому, являются результатом определенных психологических функций или связаны с определенными социальными нормами, а не с электрохимическими процессами в мозге. В данном случае мы имеем дело с психическими и поведенческими феноменами, которые невозможно описать исключительно в терминах неврологии. Например, депрессию принято считать специфическим психическим симптомом, и страдание от депрессии зависит исключительно от проявления этого симптома. Даже если бы было известно (а это не так), что все симптомы депрессии тесно связаны с химическим дисбалансом на уровне нейромедиаторов, различие между психической и мозговой дисфункцией сохранялось бы (Bublitz & Merkel, 2014). Исходя из этой логики, было показано, что психические нарушения нельзя лечить так же, как повреждения головного мозга. В противном случае можно было бы забыть обо всех достижениях современного уголовного права и принять римскую концепцию иниурии, которая охватывала любые преступления, совершенные против личности. Таким образом, специалисты высказываются за определение психических состояний, подлежащих правовой защите и за введение конкретных нормативных положений, предусматривающих наказание за посягательство на психическую неприкосновенность, а не за адаптацию и расширение защиты физической неприкосновенности.

[24] Fernanda Palma, M. (2021–2022). Ciberneurodireito. Powerpoint Presentation. Short Course in Criminal Law on Artificial Intelligence and Artificial Intelligence in Criminal Law. FDUL. IDPCC/ CIDPCC, 4. Pp. 6–14.

В то время как понятие неприкосновенности мозга должно охватывать физические вмешательства, т. е. повреждение мозга (независимо от психических последствий), понятие психической неприкосновенности должно охватывать психические вмешательства, т. е. психические повреждения независимо от последствий для мозга (Bublitz & Merkel, 2014).

В этой связи также утверждается, что психическая неприкосновенность должна предусматривать защиту от психологических манипуляций/вмешательств, таких как провоцирование эмоций, манипулирование предпочтениями и процессами принятия решений, оптимизация неконсенсусного неврологического развития, манипулирование памятью и волей, другие когнитивные и эмоциональные феномены (Bublitz & Merkel, 2014). Во всех этих случаях манипуляции/вмешательства ограничивают возможности психики или изменяют личные предпочтения и волевые функции. Однако на сегодняшний день ни одна из этих манипуляций/вмешательств, по-видимому, в целом не подпадает под действие правил, защищающих физическую неприкосновенность и психическое здоровье. Причина этого не в последнюю очередь в том, что все эти манипуляции/вмешательства вызывают только психологические изменения и не отвечают критериям причинения физического вреда. Поскольку жертва не страдает от каких-либо повреждений головного мозга и не испытывает физической боли или дискомфорта, незаконность этих манипуляций/вмешательств обусловлена их чисто психологическими последствиями (Bublitz & Merkel, 2014). В условиях развития цифровых технологий и искусственного интеллекта все указывает на то, что в будущем нейробиологические доказательства будут играть все более важную роль в установлении и раскрытии истины в случае судебных разбирательств, связанных с мозгом и психической целостностью (Shen, 2013). При этом не имеет значения, сохранится ли отрицание дуализма сознания и мозга. По этой причине, прежде чем мы перейдем к анализу нейрохакинга как такового, необходимо высказать некоторые соображения относительно текущего обсуждения юридической автономии преступлений против психической целостности и преступлений против физической неприкосновенности.

1.4. Правовая автономия преступлений против психической целостности в сравнении с преступлениями против физической целостности

Как было показано в предыдущем разделе, нейробиология и наука о данных и искусственном интеллекте не только подвергают сомнению предположения о роли психики в естественном мире, но и побуждают к переосмыслению ее роли в мире права. Получается, что в настоящее время закон обеспечивает одностороннюю защиту, поскольку он систематически защищает тело и мозг и лишь фрагментарно – разум и психические состояния. Как объяснялось в предыдущем разделе, фундаментальный вопрос заключается в том, в какой степени возможно законное вмешательство в сознание и психические состояния других субъектов. В связи с коммерциализацией и массовым внедрением нейронных технологий, способных воздействовать на сознание и обнаруживать психическую активность, многие специалисты утверждают, что закон должен предусматривать автономную и индивидуальную правовую защиту психической неприкосновенности (Bublitz & Merkel, 2014; Abegão Alves, 2020). Эта научно-философская и юридическая дискуссия в основном сосредоточена на двух аспектах: (i) рассмотрении эмпирической и концептуальной автономии

психического по отношению к физическому; (ii) рассмотрении юридической автономии преступлений против психической неприкосновенности по отношению к преступлениям против физической неприкосновенности. Так, в Институте уголовного права и криминологических наук юридического факультета Лиссабонского университета ведется научный проект «Преступления против психики» (инициированный после публикации новаторского исследования Bublitz & Merkel, 2014), целью которого является восполнение этого пробела в правовом мышлении. Исследование показало, что юристы и мыслители в области права пока не установили пределов законного изменения психического состояния других людей, так что проблемы регулирования реальности по-прежнему опережают развитие юридической науки. Также, согласно этому проекту, самые последние научные открытия требуют внимания закона не только с точки зрения агрессора/преступника, но и с точки зрения жертвы. В связи с этими открытиями юридическая наука должна обсуждать как проблему свободы воли, так и основания уголовной ответственности, а также вопросы законных активов, подлежащих защите. Именно этот второй аспект значимости нейробиологии для юриспруденции еще предстоит изучить. В этом смысле текущая задача состоит в том, чтобы углубить научно-философские и юридические дебаты по этому вопросу как на национальном, так и на международном уровне. В частности, необходимо проблематизировать ключевые вопросы, предлагая решения и возможные пути для будущих исследований, которые неизбежно будут находиться на пересечении различных областей знаний.

2. От киберпреступности к нейрохакингу

2.1. Прототипы нейропреступлений, которые обычно относят к нейрохакингу

За последние несколько лет было выявлено множество видов нейропреступлений, обычно называемых нейрохакингом. К ним относятся взлом программного обеспечения беспроводных протезов конечностей, злонамеренное перепрограммирование устройств нейростимуляционной терапии (т. е. несанкционированное беспроводное изменение конфигурации устройства с целью генерирования определенных мозговых стимулов) и несанкционированный перехват сигналов мозговых имплантатов с целью получения частной нейронной информации (Ienca & Haselager, 2016)[25]. Все это может быть выполнено только с использованием нейронных устройств, которые позволяют установить прямую связь с мозгом, таких как tDCS и особенно все более усовершенствуемый ИМК (Denning et al., 2009). Это прототипы нейропреступлений, которые обычно называют нейрохакингом. Далее мы покажем, что способ их осуществления очень похож на компьютерный взлом в контексте киберпреступности, как описано в разделе 1.1 о связи между киберпреступностью и нейропреступностью (Ienca & Haselager, 2016).

2.2. Понятие нейрохакинга

[25] Этот последний пример описывает специфический нейрокриминальный феномен, при котором атака направлена не просто на вывод нейронного устройства из строя, но и на получение несанкционированного доступа к частной информации.

В широком смысле нейрохакинг можно определить как неправомерное и злонамеренное использование нейронных устройств с целью незаконного получения нейронной информации и возможного манипулирования ею (Ienca & Haselager, 2016). Строго говоря, нейрохакинг представляет собой нейроатаку, осуществляемую с помощью нейронных устройств, в ходе которой злоумышленники получают незаконный доступ к нейронной информации, которой, в свою очередь, можно манипулировать, чтобы контролировать когнитивный процесс или выполнение определенной умственной задачи пользователем устройства. После того как доступ к нейронному устройству получен, оно используется для совершения преступлений с ведома пользователя или без него.

2.3. Нейрохакинг на основе различных типов приложений интерфейса «мозг – компьютер»

2.3.1. Масштаб проблемы

Как уже говорилось, ИМК могут быть перехвачены для обнаружения скрытой автобиографической информации пользователей с высокой степенью точности (Ienca & Haselager, 2016; Rosenfeld et al., 2006; Rosenfeld, 2011). Было показано, что перехваченный ИМК дает доступ к личной и конфиденциальной информации пользователей, например, PIN-кодам, данным банковских и кредитных карт, дате рождения, домашнему адресу, фотоснимкам знакомых им людей (Ienca & Haselager, 2016). Таким образом, фантастическое будущее уже не кажется вымыслом. Уже сейчас можно получать доступ к нейронной информации других людей и манипулировать ею (Mochan et al., 2025). Ниже мы показываем, что если конструктивные и функциональные характеристики современных нейронных устройств, которые все еще находятся в стадии разработки, не будут соответствовать строгим мерам нейробезопасности, их неправомерное и злонамеренное использование несет серьезные риски с точки зрения общественной безопасности (Ienca & Haselager, 2016)[26].

2.3.2. Приложения интерфейса «мозг – компьютер», которые могут стать целью нейрохакинга

Как было показано в разделе 2.1, в прототипах нейропреступлений используются нейронные устройства, позволяющие установить прямую связь с мозгом, а основными мишенями для взлома являются приложения ИМК. Выделяют четыре основных типа приложений ИМК, которые возможно использовать для нейрохакинга: (i) нейромедицинские приложения; (ii) приложения для аутентификации пользователей; (iii) видеоигры и развлечения и (iv) приложения на базе смартфонов. Для каждого из этих типов в настоящее время изучаются возможные сценарии атак, а также соответствующие меры нейробезопасности, которые необходимо применять (Mochan et al., 2025). На самом деле для некоторых приложений ИМК и соответствующих видов нейрохакинга уже имеются фактические данные и экспериментальные подтверждения их использования в реальных контекстах (Li et al., 2015). Как мы увидим в следующем

[26] Martinovic, I. et al. (2012). On the feasibility of side-channel attacks with brain-computer interfaces. USENIX security symposium. https://clck.ru/3NkoD5

разделе, в рамках этих четырех основных типов нейрохакинг может осуществляться на любой фазе цикла ИМК, описанных в разделе 1.2.

2.4. Модальности нейрохакинга, основанные на четырехчастном цикле интерфейса «мозг – компьютер»

2.4.1. Масштаб проблемы

Принимая во внимание описанные типы приложений ИМК, которые уже существуют в настоящее время (Mochan et al., 2025) и которые теоретически могут появиться в ближайшем будущем, рассмотрим, также теоретически, различные типы нейрохакинга, основанные на четырехфазном цикле ИМК. Напомним, что это фаза ввода нейронной информации, фаза измерения и регистрации мозговой активности, фаза декодирования и классификации нейронной информации и, наконец, фаза вывода (Ienca & Haselager, 2016).

2.4.2. Манипуляции на этапе ввода нейронной информации

При этом типе нейрохакинга хакер атакует пользователя ИМК в момент ввода нейронной информации, т. е. на первом этапе цикла. Вводом нейронной информации можно манипулировать, изменяя стимулы, передаваемые пользователю ИМК. Например, нейрохакеры могут заранее выбирать целевые стимулы, чтобы вызвать определенную реакцию у пользователя и таким образом облегчить доступ к его нейронной информации. Этот тип нейронных вредоносных программ имеет некоторое сходство со шпионскими программами на компьютере, поскольку они направлены на сбор информации о пользователе, отправку ее другому объекту и/или обеспечение контроля над компьютером или другим ИТ-устройством без разрешения или согласия пользователя (Ienca & Haselager, 2016). В этом случае вредоносное ПО, используемое для нейрохакинга, обладает способностью извлекать информацию непосредственно из сигналов, излучаемых мозгом, и поэтому широко известно как «программа-шпион для мозга». В будущем, по-видимому, появятся различные мобильные и портативные приложения для нейрошпионажа, и такие действия, как взлом паролей, кража личных данных, фишинг и другие виды нейронного мошенничества, будут все более распространенными (Ienca & Haselager, 2016). В настоящее время расшифровка сигналов мозга с уровнем точности и скорости, сравнимым с компьютерным взломом, возможна только в экспериментальной среде и лишь в ограниченных масштабах. Учитывая ограничения в плане расшифровки сигналов мозга, а также текущую степень зрелости рынка, вознаграждение для современного хакера, по-видимому, не стоит риска. Однако с развитием технологий и быстрым расширением рынка приложений для ИМК нейронная информация будет все больше цениться, а также появятся возможности для ее расшифровки (Ienca & Haselager, 2016).

2.4.3. Манипуляции на этапе измерения и записи мозговой активности

На этапе измерения и регистрации мозговой активности хакер атакует пользователя ИМК без его согласия или волеизъявления с целью получить результат, отличный от того, который ожидается при обычном функционировании нейронного устройства. Форма атаки может отличаться в зависимости от ее конкретной цели, при этом учитываются три основные цели: взлом исходных нейронных данных из ИМК (т. е. нейронной информации), нарушение функциональности и захват интерфейса

«мозг – компьютер». В целом взлом необработанных данных может вести к различным преступным действиям, направленным на ограничение определенного поведения пользователя нейронного устройства, нанесение вреда или использование преимуществ. Нарушение функциональности ИМК может производиться с целью манипулирования данными о мозговой активности, чтобы изменить, перегрузить или замедлить работу приложения ИМК. Хакер атакует канал связи интерфейса «мозг – компьютер», чтобы отслеживать или изменять данные, снизить или перехватить контроль пользователя над приложением ИМК. Во время взлома нейронное устройство получает приказы, которые расходятся с намерениями или желаниями его пользователя, и действует в интересах хакера. Например, нейрохакер может отключить устройство для воспроизведения речи, основанное на ИМК, чтобы заставить пользователя замолчать, или взломать интерфейс инвалидной коляски, чтобы определить маршрут пользователя (Ienca & Haselager, 2016).

2.4.4. Манипуляции на этапе декодирования и классификации нейронной информации

Нейрохакинг на этапе декодирования и классификации нейронной информации включает в себя манипулирование получением результата, ожидаемого пользователем, в процессе обычной обработки данных устройством ИМК. Это может быть сделано тремя различными способами: (i) путем добавления шума, что делает процесс декодирования излишне сложным; (ii) путем вмешательства в механизмы нейронного обучения и памяти (машинное обучение), чтобы изменить классификацию мозговых волн или (iii) путем замены волн, посылаемых по ИМК к устройству вывода. Каждый из этих методов имеет свои преимущества и недостатки. Например, добавление шума представляется наиболее простым в исполнении и наиболее трудным для обнаружения методом. Однако при его использовании шансы хакера на достижение желаемого результата снижаются. С другой стороны, два других метода более сложны в исполнении и их легче обнаружить, однако они обеспечивают максимальный контроль над системой ИМК. Как и при манипулировании фазой измерения и записи мозговой активности, хакер может манипулировать фазой декодирования и классификации, чтобы захватить контроль над устройством ИМК. При таком типе атаки цель состоит не только в том, чтобы ограничить или отобрать у пользователя контроль над устройством, но и в том, чтобы заменить его. Успешно взломав систему, хакер может получить частичный или полный контроль над устройством ИМК, одновременно ограничивая или устраняя контроль пользователя. В этом сценарии хакер получает возможность отслеживать, изменять или вставлять сообщения в канал связи ИМК (Ienca & Haselager, 2016).

2.4.5. Манипуляции на этапе вывода результата

В этом случае целью взлома является изменение результатов, воспринимаемых пользователем в конце цикла интерфейса «мозг – компьютер». Нейрохакер манипулирует восприятием непосредственно предшествующих действий или собственным самовосприятием пользователя, возникающим в результате когнитивных состояний, генерируемых ИМК. Преступный мотив, стоящий за этим типом взлома, заключается в том, чтобы без разрешения пользователя вызвать определенные когнитивные состояния или действия в последующем цикле (или во всех последующих

циклах) в интересах хакера. Например, нейрохакер может осуществлять своего рода «нейрофишинг»: заставить пользователя ввести определенный пароль или другой тип аутентификационной информации, чтобы начать или продолжить первоначально запланированный процесс. В этом случае, по-видимому, пользователь подвергается определенным травмирующим переживаниям. Преступные действия, которые подпадают под эту категорию, среди прочего включают мошенничество, фишинг, кражу личных данных и нанесение ущерба физической или психологической неприкосновенности (Ienca & Haselager, 2016).

3. Нейрохакинг в эпоху цифровизации и искусственного интеллекта

3.1. Концепция эпохи цифровизации и искусственного интеллекта

Эпохой информатизации обычно называют период 50–70-х гг. XX в., который характеризуется тем, что традиционные отрасли промышленности, созданные во время промышленной революции, трансформировались в экономику, основанную на информационных и коммуникационных технологиях. Сегодня, в начале XXI в., когда экономика переходит на цифровые технологии и искусственный интеллект, мы вступили в новый исторический период, а именно в эпоху цифровых технологий и искусственного интеллекта. Как упоминалось во введении, с развитием Web 1.0, Web 2.0 и Web 3.0, а в последнее время и Web 4.0 появились новые прорывные технологии, и использование цифровых и ИИ компьютерных систем расширяется все более быстрыми темпами. Среди этих новых прорывных технологий выделяются последние достижения в области иммерсивных технологий, метавселенных и виртуальных миров, а также в области искусственного интеллекта и науки о данных. В первой из этих областей выделяются технологии виртуальной (VR), дополненной (AR), смешанной (MR) и расширенной (RX) реальности, а также пространственные вычисления и цифровое сенсорное взаимодействие. Во второй области это в основном системы искусственного интеллекта и робототехники[27]. Обе эти области обещают произвести революционные изменения во взаимодействии общества и технологий. Эти типы технологий не только направлены на повышение эффективности взаимодействия с пользователями, но и обладают функциями и характеристиками, позволяющими развивать множество отраслей с головокружительной скоростью (Ford, 2016)[28] и темпами, превосходящими все прогнозы[29], в том числе в секторах, связанных с другими

[27] См. GPT-4. https://clck.ru/3NkoQK; Bing AI. https://clck.ru/3NkoTY; Gemini. https://clck.ru/3NkoV7. См. также достижения в области человекоподобных роботов, в частности: Boston Dynamics. https://clck.ru/3NkoY3; Tesla. https://clck.ru/3Nkxk8

[28] В этой связи следует отметить, что наиболее известным способом измерения прогресса в вычислительной мощности компьютеров является закон Мура. Гордон Э. Мур (Gordon E. Moore) предсказал, что каждые 18 месяцев количество транзисторов на микросхемах будет увеличиваться на 100 %. Однако информационные технологии выходят за рамки этого прогноза. Например, в отличие от аппаратного обеспечения, в котором значительно увеличился объем компьютерной памяти и объем цифровой информации, которую можно передавать по волоконно-оптическим кабелям, эффективность определенных алгоритмов в программном обеспечении растет темпами, превосходящими все прогнозы (Ford, 2016).

[29] Coelho, D. P. (2023). Os recentes avanços no setor da IA são uma benção ou uma maldição? Observador. https://clck.ru/3NkpED

прорывными достижениями, такими как облачные и передовые технологии, большие данные, квантовые вычисления, интерфейсы «мозг – компьютер», технологии распределенных реестров (такие как блокчейн), интернет вещей (IoT), умные города, распознавание лиц, робототехника и др.

Представьте, что эти технологии достигнут прогнозируемого потенциала (Dwivedi et al., 2022)[30]. В ближайшие 15–20 лет все процессы окажутся напрямую связаны. В метавселенной в цифровой форме будут созданы новые миры и страны[31]. Умные города будут подключены к интернету вещей, на каждом углу будут установлены камеры видеонаблюдения[32], оснащенные системами распознавания лиц и интеллектуальными сенсорными системами[33]. Дроны на базе искусственного интеллекта и гуманоидные роботы-полицейские будут патрулировать улицы и здания[34]. Университеты будут в основном работать на искусственном интеллекте[35]. В большинстве организаций не будет даже работников или физических помещений, поскольку они будут автономными, цифровыми и основанными на ИИ[36]. Бизнес в метавселенной станет цифровым и будет развиваться автономными цифровыми и ИИ-компаниями[37]. Промышленные роботы на базе ИИ будут производить все виды товаров[38]. Рабочие места будут практически полностью цифровыми[39]. Люди будут проводить практически весь свой день (и ночь) во все более развивающейся метавселенной[40]. Люди смогут по своему усмотрению выходить в физическую среду в виде голограмм, что позволит посещать собрания и рабочие места и даже свободно «перемещаться» в любую точку планеты[41]. И все это, разумеется, не выходя из

---

30 См. также Coelho, D. P. (2023). Ano 2050: Era Digital. Observador. https://clck.ru/3NkpRV; Chayka, K. (2021). We already live in Facebook's metaverse. The New Yorker. https://clck.ru/3NkjZb

31 См. Woodward, W. (2024). Backup nations: countries making digital twins to mitigate natural disasters. Nesta. https://goo.su/uVSUy; Widlund J. (2023) Singapore's First Country-Scale Digital Twin and The Future of Digital Open Data. https://clck.ru/3NkxqG

32 Также называемые телевидением замкнутого контура.

33 Davis, D. (2021). Facial Recognition And Beyond: Journalist Ventures Inside China's 'Surveillance State'. NPR. https://clck.ru/3NkjET

34 См. Jarecki, J., Wilson, N., & Trevellyan, K. (2024). Vermont police are using drones more than ever. Here's what that means. Vermont Public. https://clck.ru/3NkjGh ; Chen, H. (2023). Robôs com mais de 2 metros de altura integram força policial de Singapura em aeroporto. CNN Brazil. https://goo.su/W2x0

35 Carroll, M. (2024). UK's first 'teacherless' AI classroom set to open in London. Sky News. https://clck.ru/3NkjLK

36 Smith, T. (2024). Profitable, AI-powered companies with no employees to arrive 'next year'. Sifted. https://clck.ru/3NkjNX

37 Eckert, T., & Cigaina, M. (2023). The metaverse: A new space for business. SAP. https://clck.ru/3NkjPh

38 См. Ping, Ch. (2019) Robots to wipe out 20 million jobs around the world by 2030: Study. https://clck.ru/3Nkxtp; Semuels, A. (2020). Millions of Americans Have Lost Jobs in the Pandemic – And Robots and AI Are Replacing Them Faster Than Ever. Time. https://clck.ru/3Nkxxo

39 Hoover, A. (2024) The Metaverse Was Supposed to Be Your New Office. You're Still on Zoom. https://clck.ru/3Nky4S

40 Steele, C. (2022). People Are Spending More Time Online-and They're Not Happy About It. PC Mag. https://clck.ru/3NkzDa

41 См. Atkinson, E., & Meyer, M. (2022). Meeting in the Metaverse: The Future of Work?. University of Denver, Podcast. News. https://clck.ru/3Nkpxk. Verdict. In the metaverse, holograms offer more options than avatars. (2022, June 15). https://clck.ru/3Nkq2b

дома. Граница, отделяющая виртуальную реальность от дополненной и смешанной, станет менее выраженной, как и граница, отделяющая физическую реальность от цифровой. Цифровая валюта центрального банка станет единственным законным платежным средством[42]. В повседневных задачах людям будут помогать портативные и носимые технологии (во многих случаях невидимые)[43] или даже домашние роботы-гуманоиды, работающие на искусственном интеллекте[44]. В принятии решений будут участвовать голосовые помощники или даже технологии нейронного интерфейса, что позволит объединить человеческое сознание с искусственным интеллектом в своего рода симбиозе человека и машины[45]. Таким образом, при любом контакте человека с метавселенной будет инициироваться нейронная связь[46]. Цифровое сенсорное взаимодействие позволит людям чувствовать себя все более комфортно, подключаясь к метавселенной, и это реальность, которую новые поколения будут знать лучше всего. Человек всегда будет окружен камерами, микрофонами и интерфейсными системами. Даже эмбриональное развитие будет происходить в искусственных инкубаторах[47]. Многие предпочтут создавать и развивать эмоциональные или любовные отношения с домашними роботами-гуманоидами на основе искусственного интеллекта[48]. Домашних животных заменят искусственные питомцы[49]. Весь мир будет цифровым или основанным на искусственном интеллекте.

Само мышление станет небезопасным, потому что всякий раз, когда устанавливается связь с метавселенной и/или активируется технология нейронного интерфейса любого типа, человек становится открытой книгой. В этом случае использование компьютерных систем не ограничивается социальной, профессиональной и экономической сферами, а распространяется на психологическую и биологическую сферы. Ошеломляющая скорость развития этих областей, а также сочетание этих технологий неизбежно приведут к столь же ошеломляющему увеличению масштабов и скорости распространения киберпреступлений, нейропреступлений, а значит, и методов нейрохакинга. Таким образом, и как мы увидим в следующем разделе, исследования и инвестиции в кибербезопасность и нейробезопасность станут еще более актуальными (Pooyandeh et al., 2022).

---

42 Michel, N. (2024, June 17). CBDCs Are Instruments Of Control-And They're Here. Forbes. https://clck.ru/3Nkq5h

43 From Wearables to Implantables: The Rise of Invisible Technologies. https://clck.ru/3NkyPr

44 См. Reuters. (2024). A humanoid robot to help you around the house. https://clck.ru/3NkqCB; Schwartz, R. (2024). Is the world ready for Tesla's new domestic robots? The Week. https://clck.ru/3NkqE8

45 См. Brodsky, S. (2024, August 27). AI voice assistants evolve, promising deeper interaction. IBM. https://clck.ru/3NkqHZ; Niemeyer, K. (2024, August 3). Elon Musk says Neuralink could help humans compete with AI: 'Let's give people superpowers'. Business Insider. https://clck.ru/3NkqLa

46 How BCI can elevate the AR/VR experience. https://clck.ru/3NkyXe

47 Zimmer, K. (2021, March 30). The Ultimate Incubator: The Brave New World of Bionic Babies – Artificial placentas could improve the survival odds of premature infants. IEEE Spectrum. https://goo.su/PE2QYzM

48 См. Travers, M. (2024, March 24). A Psychologist Explains Why It's Possible To Fall In Love With AI. Forbes. https://clck.ru/3NkqXn; Chow, A. (2023). AI-Human Romances Are Flourishing-And This Is Just the Beginning. Time. https://clck.ru/3NkyiH

49 World Economic Forum. (2023). Moflin, an AI pet, responds like a real animal. https://clck.ru/3Nkqgf

3.2. Концепция метавселенной

В 1992 г. писатель-фантаст Нил Стивенсон в своем киберпанковском романе «Лавина» ввел термин «метавселенная». В нем он показывает трехмерный виртуальный мир, в котором люди, представленные в виде аватаров, взаимодействуют друг с другом и с искусственным интеллектом. В 2003 г. эта первоначальная концепция метавселенной (все еще далекая от концепции, идеализируемой в настоящее время) была впервые реализована в игре Second Life и даже имела некоторый успех[50]. Термин «метавселенная» образован путем сочетания греческого префикса «мета», который можно перевести как «запредельный» или «трансцендентный», и корня «verse», который происходит от слова «вселенная». Таким образом, мы имеем дело с миром, находящимся за пределами Вселенной (Bernal et al., 2022). Эта концепция направлена на представление виртуального (цифрового) мира, который, сосуществуя с физической реальностью (посредством дополненной реальности), позволяет нам преодолевать физические ограничения реального мира, такие как пространство и время. В этой цифровой среде (которая в будущем станет приобретать все большее значение) множество пользователей взаимодействуют друг с другом так же, как в реальной жизни, используя аватар, представляющий их цифровое альтер эго или их цифровую идентичность (Bernal et al., 2022). Таким образом, в широком смысле метавселенная состоит из пространства или набора виртуальных и совместно используемых пространств (обычно называемых цифровыми или виртуальными мирами или средами), к которым пользователи, представленные цифровыми аватарами, получают доступ и с которыми они взаимодействуют многомерным образом, используя гарнитуры или другие аксессуары. Другими словами, вместо простого просмотра контента пользователи могут погрузиться в него с помощью своих цифровых представлений[51].

Основными технологиями, которые в настоящее время составляют метавселенную и виртуальные миры, являются технологии погружения (виртуальная, дополненная, смешанная и расширенная реальность, ИМК и системы сенсорного взаимодействия), технологии 3D-моделирования и реконструкции, пространственные и пограничные вычисления, искусственный интеллект и наука о данных, IoT и технологии распределенного реестра (Pooyandeh et al., 2022)[52]. В отличие от современных технологий виртуальной и/или дополненной реальности, которые в основном используются для электронных игр или для замены клавиатуры, сенсорного экрана или компьютерной мыши, технологии будущего могут быть использованы для моделирования практически любой ситуации, связанной с физическим миром. Возможности

[50] Second Life – это видеоигра, выпущенная в 2003 г., позволяет пользователям наслаждаться «второй жизнью» в виртуальном мире. Пользователи могут стать любой личностью и играть любую роль. В частности, они могут играть роль аватара в виртуальном мире, исследовать его, знакомиться с другими пользователями, принимать участие в индивидуальных и/или групповых мероприятиях и так далее, как это было бы в реальной жизни. См. веб-сайт видеоигры Second Life. https://clck.ru/3Nm4mQ

[51] Pereira Coelho, D. (2021). Metaverse: should regulators be more attentive than ever? Observador. https://clck.ru/3Nm549

[52] См. также Tucci, L. (2024, March 22). What is the metaverse? An explanation and in-depth guide. TechTarget. https://clck.ru/3Nkqqk

для взаимодействия будут охватывать самые разные сферы – от профессиональной деятельности до посещения виртуальных концертов[53] или просто приятного времяпрепровождения с друзьями. Таким образом, конечная цель состоит в том, чтобы устранить границы между физическим миром и виртуальной реальностью, позволяя пользователям взаимодействовать с виртуальными объектами через объекты физического мира и наоборот. В результате человек получает возможность обрабатывать любую информацию в режиме реального времени.

Используя технологию распределенного реестра, пользователи могут покупать и продавать невзаимозаменяемые криптоактивы с помощью взаимозаменяемых криптоактивов в метавселенной. Фактически в рамках «виртуального мира, основанного на блокчейне», функционирующего на основе «виртуальной экономики», криптоактивы, выпущенные с использованием технологии блокчейн, являются цифровым представлением взаимозаменяемых финансовых продуктов. Кроме того, они являются цифровым представлением взаимозаменяемых нефинансовых продуктов, будучи как твердыми активами, т. е. осязаемыми и физическими, так и мягкими, т. е. нематериальными или цифровыми товарами. В этом смысле возможности практически безграничны, и есть мнение, что метавселенная представляет собой следующее поколение Интернета (Pooyandeh et al., 2022). Так или иначе, метавселенная, по-видимому, является, по крайней мере, развитием Интернета с преобладающим акцентом на социальное взаимодействие. По мере развития метавселенной и увеличения числа пользователей все больше личной информации, включая нейронную, будет подвергаться риску, как мы увидим в следующих разделах (Pooyandeh et al., 2022).

3.3. Цифровое сенсорное взаимодействие в метавселенной

В настоящее время, помимо взаимодействия с экраном смартфона, планшета или другого устройства посредством прикосновения, сенсорное взаимодействие с цифровой средой обычно ограничивается слухом и зрением, т. е. в общей сложности тремя из пяти традиционно известных органов чувств человека. Похоже, что в ближайшем будущем взаимодействие может включать в себя более базовые органы чувств, и их восприятие будет все больше походить на восприятие физического мира. В 2013 г. Google опубликовала поисковую систему Google Nose, которая позволяет находить нужный объект с помощью обоняния[54]. Хотя этот сервис был создан как своего рода первоапрельская шутка и для конкретных условий того времени, он был признан успешным. В то же время стало ясно, что пользователи готовы вывести взаимодействие с Интернетом на новый уровень[55]. С тех пор были разработаны удобные для пользователя цифровые сенсорные системы, позволяющие включить обоняние в сферу обычного взаимодействия с цифровой средой. Например, пользователи цифровой среды могут понюхать духи, прежде чем приобрести их в Сети. Цель состоит в том, чтобы пользователи, выйдя из дома,

---

53 Simões Ferreira, R. (2022, Desember 29). With holograms or in the metaverse, how digital has already reinvented ‘live’. Jornal de Notícias. https://clck.ru/3Nkqum

54 См. веб-сайт компании Google Nose Beta: https://clck.ru/3Nkqw4

55 Nordyke, K. (2023). Google’s April Fools’ Joke: Search and Smell (Video). The Hollywood Reporter. https://goo.su/UBRW9

могли вдохнуть запах моря, как будто они находятся на пляже, или даже ощутить влагу на своей коже. То же самое касается вкуса и ощущения аромата. В 2020 г. в Университете Мэйдзи в Японии был разработан прототип (получивший название «Дегустатор»), который позволяет пользователю ощутить различные вкусы с помощью устройства, адаптированного для прикосновения языком[56]. В этом смысле в контексте сенсорного взаимодействия пользователей с цифровой средой все чаще используются понятия «дополненный человек» или «дополненный человеческий интеллект».

В рамках метавселенной мобильные и носимые устройства, такие как, например, гарнитуры виртуальной и/или дополненной реальности, кроме датчиков, позволяющих пользователю обнаруживать движение или звук, могут также включать в себя датчики других типов. В частности, системы виртуальной реальности состоят из инерциальных измерительных устройств и включают акселерометры, гироскопы и магнитометры. Также существуют датчики времени, дыхания и освещенности. Системы дополненной реальности определяют местоположение пользователя и то, что он видит или слышит. Большинство гарнитур оснащены датчиками времени полета (time-of-flight, ToF), поверхностно-излучающими лазерами с вертикальным резонатором (vertical cavity surface-emitting laser, VCSEL), бинокулярными датчиками глубины и оптическими датчиками для изучения структур. Обе системы могут также работать с датчиками звука, такими как направленные микрофоны, а также с тепловыми датчиками, сенсорными датчиками, передними и задними видеокамерами. Сенсорные датчики используются для обмена информацией между людьми и машинами в форме человеко-машинного интерфейса, при этом активируется тактильный стимул (как, например, в сенсорной панели). Большинство из этих датчиков используются в интернете вещей в промышленности, медицине, в беспилотных летательных аппаратах и человекоподобных роботах (Pooyandeh et al., 2022).

Однако устройства для деятельности в метавселенной, которые в настоящее время массово выпускаются на рынок, по-прежнему имеют множество ограничений (с точки зрения как аппаратного, так и программного обеспечения). Подавляющее большинство из них еще недостаточно развиты, чтобы обеспечить полное погружение в метавселенную. Восприятие ощущений в физическом мире по-прежнему более совершенно, чем в цифровом. Следовательно, подавляющее большинство платформ метавселенной не справляются с большими объемами пользовательских данных, что, в свою очередь, означает, что мы также не близки к массовому внедрению таких устройств. Лучшим примером этого является очевидный провал гарнитуры Apple Vision Pro, которая была призвана заменить клавиатуру, сенсорный экран и компьютерную мышь[57]. В этом контексте в литературе (как мы увидим в следующем разделе) ИМК признается ключевой технологией для достижения полной интеграции между пользователем и метавселенной в среднесрочной и долгосрочной

[56] Grad, P. (2020). Digital device serves up a taste of virtual food. TechXplore. https://clck.ru/3Nkr7r

[57] Mitchell, A. (2024, November 12). Apple's Vision Pro flop: Company scales back production of $3,500 VR headset amid lackluster sales, customer complaints. New York Post. https://clck.ru/3Nm5Ka

перспективе (Bernal et al., 2022)[58]. Кроме того, массовому внедрению этой новой модели сенсорного взаимодействия с Интернетом способствует разработка передовых датчиков и аппаратного обеспечения, а также других видов оборудования, связанных с метавселенной[59].

3.4. Интерфейс «мозг – компьютер» в метавселенной

Нанотехнологическая компания Neuralink Corp.[60], принадлежащая, в частности, Илону Маску[61], разработала тип ИМК, который требует нейрохирургической операции для имплантации интегральной схемы (чипа) в мозг пользователя. Это одновременно интригует и обескураживает многих потенциальных потребителей. Этот тип ИМК позволяет установить двунаправленное взаимодействие с мозгом, которое включает в себя как нейронные механизмы обучения и памяти, так и нейростимуляцию. В целом, хотя эти устройства можно использовать для восстановления способности говорить, писать и даже ходить, к ним все равно относятся с некоторым подозрением[62]. Тем не менее ученые рассматривают и обсуждают современное состояние данной проблемы, в частности, путем сравнения текущего ИМК с определенными устройствами виртуальной и/или дополненной реальности, которые представляют собой своего рода шлем с функцией снятия ЭЭГ. Было обнаружено, что проблемы с эргономикой затрудняют развитие гарнитур виртуальной и/или дополненной реальности, которые содержат слишком много датчиков ЭЭГ для мониторинга областей мозга. Считается, что гарнитуры виртуальной и/или дополненной реальности, которые смягчают воздействие шума, возникающего в результате обработки мозговых волн, по-видимому, лучше всего подходят для встраивания датчиков ЭЭГ (Orlosky et al., 2021). Также утверждают, что сочетание ресурсов и технологий, включая виртуальную и/или дополненную реальность, цифровые аватары, системы сенсорного взаимодействия и ИМК, способствует широкому внедрению метавселенных во все сферы повседневной жизни. Если это так, то это могло бы

---

58 Следовательно, осознаем мы это или нет, но в настоящее время мы являемся свидетелями быстрой и радикальной трансформации области делового и коммерческого этикета как с точки зрения продуктов и методов производства, так и с точки зрения видов услуг и способов их предоставления. Например, подсознание или сны пользователей, по-видимому, не защищены от маркетинговых кампаний или даже пропаганды. Существуют системы сенсорного взаимодействия, которые могут влиять на содержание снов пользователя с помощью стимулов, воздействующих на мозг до или во время сна. В частности, они побуждают пользователя увидеть определенный продукт или услугу во сне.

59 Genser, J., Damianos, S., & Yuste, R. (2024). Safeguarding Brain Data: Assessing the Privacy Practices of Consumer Neurotechnology Companies. The Neurorights Foundation. https://clck.ru/3NkrK7

60 Устройство ИМК, разработанное компанией Neuralink, состоит из небольшого зонда с более чем тремя тысячами электродов, соединенных гибкими проводами тоньше человеческого волоса. Это устройство может отслеживать активность 1000 нейронов головного мозга. Также создан «нейрохирургический робот», который может вводить в мозг 192 электрода в минуту. См. Galeon, D. (2017, November 22). Experts: Artificial Intelligence Could Hijack Brain-Computer Interfaces. Can we prevent AI from hacking into the human brain? Futurism. https://clck.ru/3NkrMh

61 См. веб-сайт компании Neuralink. https://clck.ru/3NkrP3

62 Hall, S. B., & Baier-Lentz, M. (2022, Februry 7). 3 technologies that will shape the future of the metaverse – and the human experience. The World Economic Forum. https://clck.ru/3NkrRf

изменить социальный опыт восприятия пространства и времени. Сочетание метавселенной и ИМК является аргументом в пользу создания новых форм социального взаимодействия и интероперабельности, что делает коммуникацию между физическим и цифровым миром еще более быстрой, эффективной и действенной, а также более прозрачной (Dwivedi et al., 2022). В дополнение к своей полезности в медицинском контексте, комбинация метавселенной и ИМК также найдет применение в других контекстах. В частности, это позволит пользователям управлять определенными объектами (материальными или нематериальными, такими как продукты робототехники или цифровые аватары), или просто наслаждаться видеоиграми или другими развлечениями с помощью своего разума, мысленного проговаривания, аутентификации с помощью мозговых волн (Bernal et al., 2022). Это сочетание также может быть использовано для когнитивной оценки, эмоционального контроля и повышения когнитивной работоспособности. В современной литературе также исследуется возможность использования ИМК для обеспечения прямой связи между мозгом разных испытуемых, используя как нейронные механизмы обучения и запоминания, так и нейростимуляцию (Bernal et al., 2022). Однако, несмотря на известную эволюцию ИМК за последние несколько десятилетий, их полная реализация в сценариях метавселенной еще не изучена так глубоко, как она того заслуживает. Некоторые проблемы все еще остаются нерешенными. Во-первых, нужно провести широкий анализ того, какой вклад ИМК могут внести в развитие метавселенной. Во-вторых, представляется необходимым измерить производительность этих систем и определить тенденции и проблемы, с которыми сталкивается ИМК при применении в сценарии метавселенной. И последнее, но не менее важное: необходимо определить проблемы, ограничения и риски, связанные с использованием ИМК в метавселенной (Bernal et al., 2022).

3.5. Нейрохакинг в метавселенной

Между Интернетом и метавселенной много общего, когда речь заходит о проблемах кибербезопасности, среди которых взлом учетных записей, фишинг, вредоносное ПО и т. д. Несмотря на различия в инфраструктуре, метавселенная (Web 3.0 и Web 4.0) представляет новые виды киберпреступлений, которые отличаются от тех, что совершаются на традиционных веб-сайтах (Web 2.0). По мере расширения использования криптоактивов и цифровых валют центральных банков хакеры будут проявлять все больший интерес к взлому метавселенной (Pooyandeh et al., 2022). В этом смысле мониторинг метавселенной и обнаружение атак на новых платформах более сложны, чем на традиционных платформах. Как было показано в предыдущих разделах, с коммерциализацией и массовым внедрением продуктов, связанных с метавселенной и виртуальными мирами, масштабы деятельности хакеров существенно возрастут. Среди основных связанных с этим рисков – появление «иммерсивных атак». Это новый тип атаки в виртуальной среде, который состоит в злонамеренном манипулировании устройством с целью нанесения физического или психического вреда пользователю или причинения ему неудобств. Также заслуживает внимания атака «человек – джойстик». Она заключается в управлении пользователями, погруженными в системы виртуальной и/или дополненной реальности в метавселенной, без их ведома или разрешения, с целью перемещения их физического тела в другое место в физическом мире. При использовании комбинации ИМК, особенно тех,

которые используются для нейростимуляции, атаки направляются на чрезмерную стимуляцию или подавление определенных областей мозга, тем самым нарушая нормальную мозговую деятельность. Ущерб, причиняемый такого рода действиями, по-видимому, способен даже воссоздать последствия нейродегенеративных заболеваний, хотя в этом отношении еще предстоит провести дополнительные исследования (Bernal et al., 2022)[63].

3.6. Интерфейс «мозг – компьютер» на основе искусственного интеллекта

Искусственный интеллект способствовал прогрессу в анализе и расшифровке нейронной активности, а также развитию сектора ИМК. За последнее десятилетие появилось множество приложений для ИМК с использованием ИИ или даже исключительно на его основе. Эти «умные» ИМК, в том числе двигательные и сенсорные, показали значительный успех в области медицины. Помимо улучшения качества жизни пациентов, они расширили спортивные возможности обычных людей и ускорили эволюцию роботов и достижений нейрофизиологии. Однако, несмотря на технический прогресс, все еще существует ряд проблем, связанных с длительностью машинного обучения, получением результатов в режиме реального времени, а также измерением и регистрацией мозговой активности в рамках работы этого нового типа ИМК. Как было показано в предыдущем разделе (и в целом в гл. III), все еще существует необходимость в дополнительных исследованиях в этом направлении (Zhang et al., 2020).

3.7. Нейрохакинг и искусственный интеллект

Хотя нет достаточных доказательств того, что современные хакерские группы обладают большим техническим опытом в управлении IoT-системами на основе искусственного интеллекта, они, по всей вероятности, уже реализуют свой огромный потенциал. Большинство из этих преступных организаций состоят из хакеров, которые умеют манипулировать любыми компьютерными системами и эксплуатировать их в злонамеренных целях. Не стоит забывать, что атаки проводятся 24 часа в сутки и из любой точки мира (Velasco, 2022). С появлением технологий ИМК, основанных на искусственном интеллекте, киберпреступники, похоже, нашли новое средство для усиления своей незаконной деятельности и, в частности, новые возможности для разработки и осуществления атак на отдельных лиц, компании и даже правительства. В литературе выдвигается множество гипотез на этот счет. Во-первых, если хакер возьмет под контроль ИМК, подключенные к большому количеству людей, он сможет манипулировать ими, заставляя проголосовать за конкретного кандидата, конкретную партию или по конкретному вопросу, тем самым тайно подчиняя себе правительство и/или всю инфраструктуру государства. На данный момент это кажется в высшей степени невероятным сценарием, но не исключен риск того, что определенные хакерские группы превратят устройства ИМК в своего рода армию

[63] Стоит отметить, что и Интерпол, и Европол осведомлены о преступной деятельности, осуществляемой в метавселенной. В этой связи см. Interpol. (2022, October 20). Interpol launches first global police Metaverse. https://clck.ru/3NkriG; Europol. (2022, October 21). Policing in the metaverse: what law enforcement needs to know. https://clck.ru/3Nkrnf

программируемых роботов, готовых выполнять все команды «хозяина»[64]. Хотя ИМК были разработаны людьми для взлома человеческого мозга, существует риск того, что ИМК будет использован с той же целью искусственным интеллектом[65]. Вероятно, некоторые системы искусственного интеллекта сами могут превратиться в хакеров, как только станут «разумными» (Esmaeilzadeh & Vaezi, 2021)[66, 67]. Если это так, то все указывает на то, что в их распоряжении будут компьютеризированные средства для оценки уязвимостей любых социальных, экономических и политических систем, а затем их использования с беспрецедентной скоростью, масштабом и размахом, способами, невообразимыми для ограниченного человеческого разума. Это не просто разница в уровне интеллекта – это борьба между видами. Может даже случиться так, что некоторые системы искусственного интеллекта будут пытаться взломать другие системы искусственного интеллекта, а люди останутся лишь наблюдателями и их риски будут составлять не более чем сопутствующий ущерб. Все указывает на то, что этот сценарий не является преувеличением. На самом деле ни одна из этих гипотез не требует создания научно-фантастической технологии далекого будущего. Вовсе не кажется неразумным утверждать, что развитие искусственного интеллекта станет настолько стремительным, что даже превзойдет человеческое понимание, как, по сути, уже, кажется, и просходит[68].

Заключение

Цель нашего исследования – внести свой вклад в изучение нейрохакинга в эпоху цифровых технологий и искусственного интеллекта и, прежде всего, повысить осведомленность о последствиях для нейробезопасности (а также этических последствиях), возникающих в результате злонамеренного использования технологий нейроманипулирования, связанных с метавселенной и искусственным интеллектом.

В результате было установлено, что возможные выгоды от разработки, массового внедрения и коммерциализации такого рода технологий могут быть неадекватными возможным рискам. Как и любой компьютер, компьютерная сеть или большинство других форм информационно-коммуникационных технологий, аппаратное ядро основано на электронных компонентах, способных обрабатывать данные, т. е. записывать, обрабатывать и хранить данные (и информацию), а также выполнять алгоритмы. Таким образом, подавляющее большинство из них, в принципе, можно взломать. Стремительный технологический прогресс не является сдерживающим фактором этих процессов. Напротив, в конечном итоге он способствует им или становится вызовом. Вспомним о недавнем росте кибератак на общественные

64 Lau, J. (2020, November 18). Hacking Humans: How Neuralink May Give AI The Keys To Our Brains. Forbes. https://clck.ru/3NkrqV

65 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3NkrrW

66 Там же.

67 См. также Johnson, A. (2024, March 19). Consciousness for Artificial Intelligence? IEEE Pulse. https://clck.ru/3Nkrtg

68 Schneier, B. (2021). The Coming AI Hackers. Belfer Center for Science and International Affairs. Harvard Kennedy School. https://clck.ru/3Nkrw7

организации или росте киберпреступности в целом. В настоящее время мы наблюдаем серьезные последствия с точки зрения финансового и зачастую репутационного ущерба. Однако в ближайшем будущем, в мире «мультивселенной», состоящей из метавселенных с «умными технологиями», мы столкнемся с такими последствиями внедрения чипов в человеческий мозг для установления своего рода симбиоза с Интернетом и искусственным интеллектом, какие не в состоянии даже вообразить. Уже сегодня каждый аспект человеческой жизни отслеживается[69] и анализируется[70] мобильными устройствами (такими как смартфоны и/или умные часы), данные собираются и хранятся с целью создания подробных психографических профилей, но человеческий мозг содержит информацию, которая по самой своей природе не может быть записана без нейронного взаимодействия. Установление прямого соединения между человеческим мозгом, мобильными устройствами и искусственным интеллектом может открыть доступ к человеческому сознанию. Это также может позволить определенным группам хакеров (которые обычно на шаг опережают протоколы безопасности) взять под контроль человеческий разум, включая процесс принятия решений и их исполнение. В этом случае представьте себе последствия для процедур голосования и в контексте политических выборов или других более или менее мирных политических движений. Представьте себе неограниченные возможности для создания «суперсолдат» в условиях войн и даже для наблюдения и общественного контроля. Представьте себе в предельном и апокалиптическом сценарии будущего возможность того, что сам искусственный интеллект сможет взять под контроль нейронный интерфейс и, таким образом, человеческое сознание.

В любом случае похоже, что в ближайшем будущем будет становиться все легче внедрять идеи и даже идеологии в сознание людей (что в настоящее время происходит в основном через социальные сети). В какой степени можно будет гарантировать защиту персональных данных в случае нейроатаки? В этом контексте термин «персональные данные» приобретает совершенно новый смысл. Учитывая фрейдистскую теорию системы «восприятие – сознание», в какой степени можно гарантировать защиту самого «сознательного психического процесса», включая предыдущее бессознательное состояние? Вспомним фильм 2010 г. «Начало» с Леонардо Ди Каприо в главной роли. В этом контексте возникает также ряд философских вопросов. Что такое реальный мир? Как мы можем узнать, реален он или нет? Можно ли считать жизнь в метавселенной «более реальной», чем то, что считается реальной жизнью сегодня?

Среди самых известных предупреждений Илона Маска (которого часто считают своего рода спасителем человечества[71]) выделяются два весьма необычных. В 2018 г. он заявил, что искусственный интеллект может стать «бессмертным диктатором»[72], от которого человечество «никогда не сможет убежать». В 2020 г.

---

69 Szoldra, P. (2016, September 16). This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks. Business Insider. https://clck.ru/3Nkry8

70 Shane, S., Rosenberg, M., & Lehren, A. (2017, March 7). WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents. The New York Times. https://clck.ru/3Nkrzw

71 Dowd, M. (2017, March 26). Elon Musk's Billion-Dollar Crusade to Stop the A.I. Apocalypse. The Vanity Fair. https://clck.ru/3NkkHp

72 Holley, P. (2018, April 6). Elon Musk's nightmarish warning: AI could become 'an immortal dictator from which we would never escape'. The Washington Post. https://clck.ru/3NkkGv

он снова предупредил о той же проблеме, на этот раз заявив, что «искусственный интеллект обгонит человека менее чем за пять лет»[73]. Однако? помимо этих, мягко говоря, интригующих высказываний, Илон Маск также постоянно, упорно и без видимых ограничений стремится развивать функциональность и технологические возможности этого типа технологий, а также расширять возможные формы их применения. Впечатляют современные технологические разработки в области робототехники, созданные компанией Tesla, Inc. В частности, стоит упомянуть проект Tesla Optimus[74] и создание человекоподобных роботов по прозвищу Оптимус[75], внешний вид и характеристики которых напоминают роботов из фильма 2004 г. «Я, робот» с Уиллом Смитом в главной роли или роботов Skynet из фильма «Терминатор» 1995 г. с Арнольдом Шварценеггером. Не открываем ли мы неосознанно двери в вымышленный, мрачный мир, как в фильме «Матрица», снятом в далеком 1999 г.? Только время покажет.

Список литературы

Abegão Alves, C. (2020). Contra a mente: ensaio de integração das lesões resultantes de intervenções na mente no artigo 143.º do Código Penal. In M. Fernanda Palma et al. (org.). *Livro em Memória do Professor Doutor João Curado Neves. Associação Académica da Faculdade de Direito de Lisboa* (pp. 215–235). AAFDL Editora. (In Portug.).

Bernal, S. L., Pérez, M. Q., Martínez Beltrán, E. T., Martínez Pérez, G., & Huertas Celdrán, A. (2022). When Brain-Computer Interfaces Meet the Metaverse: Landscape, Demonstrator, Trends, Challenges, and Concerns. *Computer Science – Human-Computer Interaction*. https://doi.org/10.48550/arXiv.2212.03169

Bublitz, J. C., & Merkel, R. (2014). Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. *Criminal Law and Philosophy*, *8*, 51–77. https://doi.org/10.1007/s11572-012-9172-y

Czech, A. (2021). Brain-Computer Interface Use to Control Military Weapons and Tools. In S. Paszkiel (Ed.), *Control, Computer Engineering and Neuroscience. ICBCI 2021. Advances in Intelligent Systems and Computing* (Vol. 1362). Springer, Cham. https://doi.org/10.1007/978-3-030-72254-8_20

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: Security and privacy for neural devices. *Neurosurgical Focus*, *27*(1), E7. https://doi.org/10.3171/2009.4.focus0985

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, Bh., Buhalis, D., Cheung, Ch. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, Ch., Jebabli, I., Janssen, … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Ford, M. (2016). *Robôs: A Ameaça de um futuro sem emprego*. Bertrand Editora. (In Portug.).

Esmaeilzadeh, H., & Vaezi, R. (2021). Conscious AI. *arXiv:2105.07879*. https://doi.org/10.48550/arXiv.2105.07879

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*, 117–129. https://doi.org/10.1007/s10676-016-9398-9

Kotchetkov, I., Hwang, B. Y., Appelboom, G., Kellner, Ch. P., & Connolly E. S. Jr. (2010). Brain-computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, *28*(5), E25. https://doi.org/10.3171/2010.2.focus1027

---

73 Cuthbertson, A. (2020, July 27). Elon Musk claims AI will overtake humans 'in less than five years'. Independent. https://clck.ru/3NkkF2

74 Levin, T. (2022, January 27). Elon Musk says Tesla's humanoid robot is the most important product it's working on – and could eventually outgrow its car business. Business Insider. https://clck.ru/3NkkDD

75 Gomez, B. (2021, August 24). Elon Musk warned of a 'Terminator'-like AI apocalypse – now he's building a Tesla robot. CNBC. https://clck.ru/3NkkBk

Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges. *IEEE conference on communications and network security (CNS). Florence, 2015* (pp. 663–666). https://doi.org/10.1109/CNS.2015.7346884

Marques, G., & Martins, L. (2006). *Direito da informática* (2.ª Edição). Almedina. (In Portug.).

Miranda, R., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., Manzo, J. E., Pankratz, K. G., Pratt, G. A., Sanchez, J. C., Weber, D. J., Wheeler, T. L., & Ling, G. S. F. (2015). DARPA-funded efforts in the development of novel brain-computer interface technologies. *Journal of Neuroscience Methods*, *244*, 52–67. https://doi.org/10.1016/j.jneumeth.2014.07.019.

Mochan, A., Parkin, B., Farinha, J., & Bailey, G. (2025). *Emerging applications of neurotechnology and their implications for EU governance*. Publications Office of the European Union. Luxembourg.

Moulin, T. (2022). 'I Will Control Your Mind': The International Regulation of Brain-Hacking. *San Diego International Law Journal*, *24*(65).

Orlosky, J., Sra, M., Bektaş, K., Peng, H., Kim, J., Kosmyna, N., Höllerer, T., Steed, A., Kiyokawa, K., Akşit, K. (2021). Telelife: The Future of Remote Living. *Frontiers in Virtual Reality*, *2*, 763340. https://doi.org/10.3389/frvir.2021.763340

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences. MDPI*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Radu, R. (2024). Neurotechnologies and the future of internet governance. Technical Report. EUI. RSC (Global Governance Programme). *GIFI. Issue Brief*.

Rodrigues, B. S. (2009). *Direito Penal Especial. Direito Penal Informático-Digital*. Almedina. (In Portug.).

Rosenfeld, P., Biroschak, J., & Furedy, J. (2006). P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms. *International Journal of Psychophysiology*, *60*(3), 251–259. https://doi.org/10.1016/j.ijpsycho.2005.06.002

Rosenfeld, P. (2011). P300 in detecting concealed information. In B. Verschuere, G. Ben-Shakhar, & E. Meijer (Eds), *Memory detection: Theory and application of the concealed information test* (pp. 63–89). Cambridge University Press. https://doi.org/10.1017/CBO9780511975196.005

Shen, F. (2013). Mind, Body, and the Criminal Law. *Minnesota Law Review*, *97,* 2036–2175.

Vallabhaneni, A., Wang, T., & He, B. (2005). Brain – Computer Interface. In B. He (Ed.), *Neural Engineering. Bioelectric Engineering* (pp. 85–121). Springer. Boston, MA. https://doi.org/10.1007/0-306-48610-5_3

Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., Ramsey, N., Haselager, P., Vuurpijl, L., Gielen, S., & Desain, P. (2009). The brain-computer interface cycle. *Journal of Neural Engineering*, *6*(4), 041001. https://doi.org/10.1088/1741-2560/6/4/041001

Vasconcelos Casimiro, S. (2000). *A responsabilidade civil pelo conteúdo da informação transmitida pela Internet*. Almedina. (In Portug.).

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, *23*, 109–126. https://doi.org/10.1007/s12027-022-00702-z

Venâncio, P. (2011). *Lei do Cibercrime. Anotada e Comentada*. Almedina. (In Portug.).

Yuan, B., Hsieh, Chih-Hung, & Chang, Chien-Ching (2010). National technology foresight research: A literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy*, *6*(1), 5–35. http://dx.doi.org/10.1504/IJFIP.2010.032663

Zhang, X., Ma, Z., Zheng, H., Li, T., Chen, K., Wang, X., Liu, Ch., Xu, L., Wu, X., Lin, D., Lin, H. (2020). The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Annals of Translational Medicine*, *8*(11), PMC7327323. https://doi.org/10.21037/atm.2019.11.109

Сведения об авторе

Коэльо Диого Перейра – аспирант, Севильский университет
Адрес: Испания, 41013, г. Севилья, Калле Сан Фернандо, д. 4
E-mail: diopercoe@alum.us.es
ORCID ID: https://orcid.org/0000-0002-2082-1231
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57703490300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/GLU-8923-2022
Google Scholar ID: https://scholar.google.com/citations?user=-laUdL8AAAAJ

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 5 мая 2025 г.
Дата одобрения после рецензирования – 26 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/smgmxq
DOI: https://doi.org/10.21202/jdtl.2025.16

Neurohacking in the Digital and Artificial Intelligence Age: Legal Aspects of Protecting Neural Information

Diogo Pereira Coelho
University of Seville, Seville, Spain

Keywords

artificial intelligence,
brain-computer interface,
cybercrime,
digital technologies,
law,
metaverse,
neurocrime,
neurohacking,
neurosecurity,
neurotechnologies

Abstract

Objective: to contribute to the concept of neurocrime; to study the current and future risks from the viewpoint of cybersecurity in the context of digitalization and artificial intelligence development.

Methods: the study uses a critical and descriptive analysis of the relationship between cybercrime and neurocrime. It provides a conceptual distinction between the brain-computer interface and its use and describes the differences between neural and mental manipulation. The legal autonomy of crimes against mental integrity in relation to crimes against physical integrity is investigated. The methodological framework includes the analysis of existing prototypes of neurocrimes based on a four-phase brain-computer interface cycle and the study of the features of neurohacking in the context of the metaverse and artificial intelligence technologies.

Results: the study revealed the essential characteristics of neurohacking as the misuse of neural devices to gain unauthorized access to and manipulate neural information. Four main types of brain-computer interface applications subject to neurohacking are identified: neuromedical applications, user authentication systems, video games, and smartphone-based applications. The modalities of neurohacking were established at each phase of the brain-computer interface cycle: manipulations at the stage of neural information input, measuring and recording of brain activity, decoding and classifying neural information, as well as at the stage of the result output. The specific threats of neurohacking in the era of digitalization are analyzed, including immersive attacks and human joystick attacks in the metaverse.

Scientific novelty: for the first time, a comprehensive differentiation of the concepts of neurocrime and cybercrime was carried out, highlighting their specific legal consequences. The author proposed a classification of neurocrimes based on the four-phase cycle of the brain-computer interface. The study substantiated the need to distinguish mental integrity as an independent object of legal protection, different from the protection of physical integrity. For the first time, the features of neurohacking in the context of the metaverse and artificial intelligence technologies were investigated, including the analysis of new types of attacks and threats to neurosecurity.

Practical significance: the study results are important for the development of legal regulation in the field of cybersecurity and the corresponding regulations. The identified types of neurocrimes and their classification can help to create a specialized legislation on the protection of neural data and mental integrity. Practical recommendations on ensuring the neurosecurity of brain-computer interfaces are in demand in medical practice, video game industry, authentication systems, and for the development of smartphone applications.

For citation

Coelho, D. P. (2025). Neurohacking in the Digital and Artificial Intelligence Age: Legal Aspects of Protecting Neural Information. *Journal of Digital Technologies and Law, 3*(3), 397–430. https://doi.org/10.21202/jdtl.2025.16

References

Abegão Alves, C. (2020). Contra a mente: ensaio de integração das lesões resultantes de intervenções na mente no artigo 143.º do Código Penal. In M. Fernanda Palma et al. (org.). *Livro em Memória do Professor Doutor João Curado Neves. Associação Académica da Faculdade de Direito de Lisboa* (pp. 215–235). AAFDL Editora. (In Portug.).

Bernal, S. L., Pérez, M. Q., Martínez Beltrán, E. T., Martínez Pérez, G., & Huertas Celdrán, A. (2022). When Brain-Computer Interfaces Meet the Metaverse: Landscape, Demonstrator, Trends, Challenges, and Concerns. *Computer Science – Human-Computer Interaction*. https://doi.org/10.48550/arXiv.2212.03169

Bublitz, J. C., & Merkel, R. (2014). Crimes Against Minds: On Mental Manipulations, Harms and a Human Right to Mental Self-Determination. *Criminal Law and Philosophy*, *8*, 51–77. https://doi.org/10.1007/s11572-012-9172-y

Czech, A. (2021). Brain-Computer Interface Use to Control Military Weapons and Tools. In S. Paszkiel (Ed.), *Control, Computer Engineering and Neuroscience. ICBCI 2021. Advances in Intelligent Systems and Computing* (Vol. 1362). Springer, Cham. https://doi.org/10.1007/978-3-030-72254-8_20

Denning, T., Matsuoka, Y., & Kohno, T. (2009). Neurosecurity: Security and privacy for neural devices. *Neurosurgical Focus*, *27*(1), E7. https://doi.org/10.3171/2009.4.focus0985

Dias Venâncio, P. (2011). *Lei do Cibercrime. Anotada e Comentada*. Almedina. (In Portug.).

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, Bh., Buhalis, D., Cheung, Ch. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, Ch., Jebabli, I., Janssen, … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Ford, M. (2016). *Robôs: A Ameaça de um futuro sem emprego*. Bertrand Editora. (In Portug.).

Esmaeilzadeh, H., & Vaezi, R. (2021). Conscious AI. *arXiv:2105.07879*. https://doi.org/10.48550/arXiv.2105.07879

Ienca, M., & Haselager, P. (2016). Hacking the brain: brain-computer interfacing technology and the ethics of neurosecurity. *Ethics and Information Technology*, *18*, 117–129. https://doi.org/10.1007/s10676-016-9398-9

Kotchetkov, I., Hwang, B. Y., Appelboom, G., Kellner, Ch. P., & Connolly E. S. Jr. (2010). Brain-computer interfaces: Military, neurosurgical, and ethical perspective. *Neurosurgical Focus*, *28*(5), E25. https://doi.org/10.3171/2010.2.focus1027

Li, Q., Ding, D., & Conti, M. (2015). Brain-computer interface applications: Security and privacy challenges. *IEEE conference on communications and network security (CNS). Florence, 2015* (pp. 663–666). https://doi.org/10.1109/CNS.2015.7346884

Marques, G., & Martins, L. (2006). *Direito da informática* (2.ª Edição). Almedina. (In Portug.).

Miranda, R., Casebeer, W. D., Hein, A. M., Judy, J. W., Krotkov, E. P., Laabs, T. L., Manzo, J. E., Pankratz, K. G., Pratt, G. A., Sanchez, J. C., Weber, D. J., Wheeler, T. L., & Ling, G. S. F. (2015). DARPA-funded efforts in the development of novel brain-computer interface technologies. *Journal of Neuroscience Methods*, *244*, 52–67. https://doi.org/10.1016/j.jneumeth.2014.07.019.

Mochan, A., Parkin, B., Farinha, J., & Bailey, G. (2025). *Emerging applications of neurotechnology and their implications for EU governance*. Publications Office of the European Union. Luxembourg.

Moulin, T. (2022). 'I Will Control Your Mind': The International Regulation of Brain-Hacking. *San Diego International Law Journal*, *24*(65).

Orlosky, J., Sra, M., Bektaş, K., Peng, H., Kim, J., Kosmyna, N., Höllerer, T., Steed, A., Kiyokawa, K., Akşit, K. (2021). Telelife: The Future of Remote Living. *Frontiers in Virtual Reality*, *2*, 763340. https://doi.org/10.3389/frvir.2021.763340

Pooyandeh, M., Han, K. J., & Sohn, I. (2022). Cybersecurity in the AI-Based Metaverse: A Survey. *Applied Sciences. MDPI*, *12*(24), 12993. https://doi.org/10.3390/app122412993

Radu, R. (2024). Neurotechnologies and the future of internet governance. Technical Report. EUI. RSC (Global Governance Programme). *GIFI. Issue Brief*.

Rodrigues, B. S. (2009). *Direito Penal Especial. Direito Penal Informático-Digital*. Almedina. (In Portug.).

Rosenfeld, P., Biroschak, J., & Furedy, J. (2006). P300-based detection of concealed autobiographical versus incidentally acquired information in target and non-target paradigms. *International Journal of Psychophysiology*, *60*(3), 251–259. https://doi.org/10.1016/j.ijpsycho.2005.06.002

Rosenfeld, P. (2011). P300 in detecting concealed information. In B. Verschuere, G. Ben-Shakhar, & E. Meijer (Eds), *Memory detection: Theory and application of the concealed information test* (pp. 63–89). Cambridge University Press. https://doi.org/10.1017/CBO9780511975196.005

Shen, F. (2013). Mind, Body, and the Criminal Law. *Minnesota Law Review*, *97,* 2036–2175.

Vallabhaneni, A., Wang, T., & He, B. (2005). Brain – Computer Interface. In B. He (Ed.), *Neural Engineering. Bioelectric Engineering* (pp. 85–121). Springer. Boston, MA. https://doi.org/10.1007/0-306-48610-5_3

Van Gerven, M., Farquhar, J., Schaefer, R., Vlek, R., Geuze, J., Nijholt, A., Ramsey, N., Haselager, P., Vuurpijl, L., Gielen, S., & Desain, P. (2009). The brain-computer interface cycle. *Journal of Neural Engineering*, *6*(4), 041001. https://doi.org/10.1088/1741-2560/6/4/041001

Vasconcelos Casimiro, S. (2000). *A responsabilidade civil pelo conteúdo da informação transmitida pela Internet*. Almedina. (In Portug.).

Velasco, C. (2022). Cybercrime and Artificial Intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, *23*, 109–126. https://doi.org/10.1007/s12027-022-00702-z

Yuan, B., Hsieh, Chih-Hung, & Chang, Chien-Ching (2010). National technology foresight research: A literature review from 1984 to 2005. *International Journal of Foresight and Innovation Policy*, *6*(1), 5–35. http://dx.doi.org/10.1504/IJFIP.2010.032663

Zhang, X., Ma, Z., Zheng, H., Li, T., Chen, K., Wang, X., Liu, Ch., Xu, L., Wu, X., Lin, D., Lin, H. (2020). The combination of brain-computer interfaces and artificial intelligence: applications and challenges. *Annals of Translational Medicine*, *8*(11), PMC7327323. https://doi.org/10.21037/atm.2019.11.109

Author information

Diogo P. Coelho – PhD student, University of Seville
Address: 4 Calle San Fernando, 41013 Sevilla, Spain
E-mail: diopercoe@alum.us.es
ORCID ID: https://orcid.org/0000-0002-2082-1231
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57703490300
WoS Researcher ID: https://www.webofscience.com/wos/author/record/GLU-8923-2022
Google Scholar ID: https://scholar.google.com/citations?user=-laUdL8AAAAJ

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 5, 2025
Date of approval – May 26, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:340.1:004.8
EDN: https://elibrary.ru/pltfwo
DOI: https://doi.org/10.21202/jdtl.2025.17

Агентный искусственный интеллект: правовые и этические вызовы автономных систем

Гордон Боуэн

Университет Англия Рёскин, Кембридж, Великобритания

Ключевые слова

автономность,
агентный искусственный интеллект,
искусственный интеллект,
ответственность,
право,
правовое регулирование,
программирование,
риск,
цифровые технологии,
этика

Аннотация

Цель: определить специфические правовые и этические проблемы агентного искусственного интеллекта и выработать рекомендации по созданию защитных механизмов для обеспечения ответственного функционирования автономных ИИ-систем.

Методы: исследование носит концептуальный характер и основано на системном анализе научной литературы по вопросам этики искусственного интеллекта, правового регулирования автономных систем и социального взаимодействия ИИ-агентов. В работе применяются сравнительный анализ различных типов ИИ-систем, исследование потенциальных рисков и преимуществ агентного искусственного интеллекта, а также междисциплинарный подход, интегрирующий достижения в сфере права, этики и компьютерных наук для формирования комплексного понимания проблематики.

Результаты: установлено, что агентный искусственный интеллект, обладая автономностью принятия решений и способностью к социальному взаимодействию, создает качественно новые правовые и этические вызовы по сравнению с традиционными ИИ-ассистентами. Выявлены основные категории потенциального вреда: прямое воздействие на пользователей через открытые и скрытые действия, манипулятивное влияние на поведение и кумулятивный вред от длительного взаимодействия. Определена необходимость распределения ответственности между тремя ключевыми субъектами: пользователем, разработчиком и владельцем системы агентного искусственного интеллекта.

Научная новизна: впервые проведен системный анализ этических аспектов агентного искусственного интеллекта как качественно нового класса автономных систем, отличающихся от традиционных ИИ-ассистентов степенью независимости и социальной интерактивности. Разработана типология потенциальных рисков социального взаимодействия с агентными интеллектуальными системами, и предложена концептуальная модель распределения правовой и этической ответственности в триаде «пользователь – разработчик – владелец».

Практическая значимость: результаты исследования формируют теоретическую основу для разработки этических принципов и правовых норм регулирования агентного искусственного интеллекта в условиях растущего рынка автономных интеллектуальных систем. Полученные выводы могут быть использованы законодателями при создании нормативной базы, разработчиками при проектировании защитных механизмов, а также организациями при внедрении агентных систем искусственного интеллекта в различных сферах экономической деятельности.

Для цитирования

Боуэн, Г. (2025). Агентный искусственный интеллект: правовые и этические вызовы автономных систем. *Journal of Digital Technologies and Law*, *3*(3), 431–445. https://doi.org/10.21202/jdtl.2025.17

Содержание

Введение

В настоящее время мы наблюдаем расширение возможностей ИИ-агентов, таких как коммуникационные навыки и сложные рассуждения без вмешательства человека. ИИ-ассистенты привязаны к пользователям, но агенты с искусственным интеллектом имеют определенную степень свободы[1]. Глобальная рыночная стоимость агентного ИИ в 2024 г. составляла 5,1 млрд долл. США и, как ожидается, к 2030 г. увеличится до 47 млрд долл. США при совокупном годовом темпе роста в 44 %[2]. Степень свободы, которой в настоящее время обладают агенты с искусственным интеллектом, требует правовых и этических рамок для регулирования их поведения. Как владелец/разработчик агентного ИИ, так и соответствующее программное обеспечение нуждаются в мониторинге с юридической и этической точек зрения. Но, чтобы не потерять преимущества агентного ИИ, необходимо соблюдать баланс. Для «статичных» помощников с ИИ уже выработаны этические и правовые рамки, которые контролируются соответствующими действиями или привязаны к ним. Однако они требуют пересмотра по отношению к ИИ-агентам. Как же именно следует изменить эти рамки для агентов с ИИ? Требуется ли агентному ИИ

1 Morris, B. (2024). Beyond Intelligence: The Impact of Advanced AI Agents. https://clck.ru/3NedB2

2 Vailshery, L. S. (2025). Global market value of agentic AI 2030. https://clck.ru/3NedDe

общественное сознание, чтобы ориентироваться в новой этической и правовой среде? Главная цель нашего исследования – определить, как будут развиваться дебаты об этике и правовом поле для агентов с искусственным интеллектом. Статья состоит из введения, обзора литературы, основной части и выводов.

1. Обзор литературы

1.1. Три типа ИИ агентов

ИИ-агенты называют также сложными системами ИИ; в настоящее время эта область исследований бурно развивается (Kapoor et al., 2024). Сложные системы ИИ – это лучший способ использовать и максимизировать модели ИИ и, возможно, один из важнейших трендов 2024 г.[3] Сложные системы искусственного интеллекта во многих отношениях отличаются от обычных ИИ-систем (больших языковых моделей). Так, они решают более сложные задачи, чаще используются в реальных условиях и могут решать проблемы, на которые нет однозначного ответа; для них могут потребоваться пользовательские интерфейсы агент-компьютер (Yang, Jimenez et al., 2024). Сложная ИИ-система может управлять несколькими агентами, что сказывается на ее стоимости (Kapoor et al., 2024).

В отношении традиционного ИИ считается, что агенты способны воспринимать окружающую среду и воздействовать на нее (Russell & Norvig, 1995); с этой точки зрения термостат может быть классифицирован как агент (Kapoor et al., 2024). Агентные ИИ-системы часто рассматриваются как различные системы искусственного интеллекта с той или иной степенью агентной способности[4]. Существует три типа ИИ-агентов (Alberts, Keeling et al., 2024): артефакты (агент интерпретирует данные в социальной среде), интерактивные системы (ведут себя как социальные субъекты) и диалоговые агенты (выполняют социальные роли). ИИ-агенты как социальные субъекты должны уметь общаться и, таким образом, взаимодействовать с пользователем, но это означает нечто большее, чем просто быть приятными, дружелюбными, говорить правду и не использовать ненормативную лексику. Ожидается, что взаимодействие будет контекстуальным, что требует понимания личности пользователя, социальной среды и ситуационного контекста. Это приведет к тому, что ИИ-агенты будут выдавать информацию без запроса, а значит, вносить собственные предложения (Alberts, Keeling et al., 2024).

1.2. Социальное взаимодействие ИИ-агентов

Технологии можно считать социальными, поскольку они внедрены в социальную среду и используются в ней. Это предположение разделяют исследователи, изучающие идеологический аспект технологий, в частности, культурные предубеждения и ценности, которые заложены в используемых технологиях (Bender et al., 2021; Shelby et al., 2023). Системы, которые не являются социально интерактивными, рассматриваются как вредные (Alberts, Keeling et al., 2024). Примером вреда «пассивной»

---

[3] Zaharia, M., Khattab, O., Chen, L., Davis, J. Q., Miller, H., Potts, C., Zou, J., Carbin, M., Frankle, J., Rao, N., & Ghodsi, A. (2024). The Shift from Models to Compound AI Systems. https://clck.ru/3NedKd

[4] Ng, A. (2024). Welcoming Diverse Approaches Keeps Machine Learning Strong. https://clck.ru/3NedNZ

технологической системы служат данные об уровне обученности, которые искажают демографическую картину (Bender et al., 2021).

Помимо пассивных технологий, интерактивные технологии имеют определенное назначение и являются ценными для социума (Grimes et al., 2021). Кроме того, локальные действия системы интерпретируются с точки зрения человека и общества. На этом принципе основана философия исследования «Компьютеры как социальные субъекты», согласно которому люди, взаимодействуя с компьютерными системами и технологиями, применяют человеческие социальные нормы и ожидания (Nass et al., 1994).

Интерактивные системы имитируют поведение или качества человека. Это достигается с помощью социальных сигналов (говорение от первого лица и выражение эмоций) (Grimes et al., 2021). Диалоговые агенты способны давать адекватную реакцию в знакомых социальных ситуациях. Система ИИ может выполнять социальную роль, в которой ИИ-агент является другом или терапевтом. Однако ИИ-агент может также сказать что-то оскорбительное и расстроить пользователя, либо проявить фамильярность, что ассоциируется с презрением или бесчувственностью (Alberts, Keeling et al., 2024). Социальные взаимодействия, которые могут причинить вред, классифицируются следующим образом (Alberts, Keeling et al., 2024):

– прямой вред пользователю – побуждение к открытым действиям, таким как оскорбление из-за используемого языка или поведения;

– прямой вред пользователю – побуждение к скрытым действиям, таким как формирование мнений, которые кажутся положительными или нейтральными;

– взаимодействия, которые оказывают вредное влияние на поведение, – введение в заблуждение или предоставление ложной информации;

– взаимодействия, которые оказывают вредное влияние на поведение, – манипулирование пользователями и побуждение их делать то, чего они обычно не делают;

– взаимодействия, которые в совокупности наносят вред пользователям – вред, возникающий в процессе отношений с течением времени.

Вред от взаимодействий возникает в результате языкового воздействия (Shelby et al., 2023). Прямой вред пользователю происходит посредством контекстуального языка и языка отношений. Язык может восприниматься как более позитивный (ласковое обращение с использованием пренебрежительных выражений) или менее позитивный (покровительственное отношение к женщинам или пожилым людям) в зависимости от ситуации (Coghlan et al., 2021).

Вторичные негативные последствия возникают в ходе взаимодействий с инфлюэнсерами, то есть лицами, способными влиять на мышление или действия других людей. Таким образом, агентный ИИ может оказывать чрезмерное влияние, вызывая у пользователя несвойственное ему или неадекватное поведение (Alberts, Keeling et al., 2024). Использование социальных сигналов делает системы более интуитивно понятными и привлекательными (Kocielnik et al., 2021). Люди реагируют на социальные сигналы эмоционально, а не рационально, и это может быть использовано для манипулирования их действиями (Alberts, Lyngs et al., 2024; Shamsudhin & Jotterand, 2021).

Взаимодействия, в совокупности причиняющие вред, включают в себя пренебрежительные действия, которые воспринимаются как бестактные

и контролирующие. Коллективный эффект причинения вреда является кумулятивным, например, единичный случай бестактности может быть проигнорирован, но если он повторится, то со временем это будет иметь негативные последствия (Alberts, Keeling et al., 2024).

1.3. Принятие решений с помощью агентного ИИ

Агентные системы искусственного интеллекта требуют беспрецедентной автономии и понимания контекста (Martinez & Kifle, 2024; Mohanarangan et al., 2024). Процесс принятия решений алгоритмом агентного ИИ должен быть поистине революционным, чтобы соответствовать требованиям автономной работы и принятия логичных и последовательных решений в среде, в которой он функционирует. Алгоритм должен принимать решения в режиме реального времени и синтезировать сложные данные и массивы данных (Abuelsaad et al., 2024). Агентный ИИ обладает двумя возможностями, которые выходят за рамки возможностей ИИ-ассистентов. Во-первых, процесс принятия решений осуществляется на разных уровнях, от реагирования на низком уровне до стратегического реагирования на высоком уровне, что требует долгосрочного планирования (Abuelsaad et al., 2024). Вторая возможность – это переход от реактивного к проактивному целенаправленному поведению, которое требует от системы выявления сложных задач и определения необходимых подзадач. Таким образом, для достижения своих целей агентный ИИ требует гибкой архитектуры своего программного обеспечения для управления целями (Martinez & Kifle, 2024). Агентный ИИ должен использовать адаптивный стиль обучения. Это подразумевает освоение различных стилей обучения, а также способность ускорять процесс обучения и активно применять приемы обучения, соответствующие конкретной ситуации. При адаптивной системе обучения система извлекает уроки из прошлого опыта (Abuelsaad et al., 2024).

В деятельности организации агентный ИИ выступает в качестве стороннего исполнителя. Организация, внедряющая систему на ранних этапах, получит преимущество (положение на рынке, инновации, отношения с клиентами, операционная эффективность, уровень обучения, доля рынка). Однако при внедрении ее на поздних этапах компании потенциально потеряют свои конкурентные преимущества (снижение доли рынка и увеличение расходов; задержки при внедрении инноваций; отставание в персонализации услуг; более высокие альтернативные издержки и эксплуатационные расходы; меньше возможностей для раннего обучения; потенциально более высокий барьер для входа на рынок за счет снижения возможностей для тестирования инноваций) (Beulen et al., 2022). Агентный ИИ обладает многими преимуществами, среди которых: положительное влияние на операционные расходы; более высокая эффективность, поскольку ИИ может выполнять задачи автоматически и с большей точностью; масштабируемость без необходимости в дополнительных ресурсах и инвестициях; нацеленность на достижение поставленных целей, тогда как организация может сосредоточиться на своей основной деятельности и оставить второстепенные или менее важные задачи ИИ (Hosseini & Seilani, 2025). Однако использование агентного ИИ имеет и ряд недостатков: зависимость от технологий (чрезмерная зависимость от технологий может привести к сбоям в работе при

использовании искусственного интеллекта); ограниченный диапазон персонализации, тогда как многие задачи требуют тщательной настройки; проблемы конфиденциальности и безопасности, например, передача данных сторонним исполнителям вызывает опасения пользователей по поводу конфиденциальности и безопасности; скрытые расходы, связанные с обучением, развертыванием и внедрением систем.

В будущем приложения агентного ИИ найдут применение во многих отраслях, включая робототехнику и производство[5], системы здравоохранения[6], транспорт и логистику[7], системы управления дорожным движением[8] и финансовые услуги[9]. Одним из новых применений агентного ИИ является динамизация потребностей пациентов, что приведет к созданию персонализированных лекарств (Hasan et al., 2025). При этом агентный ИИ управляет действиями пациентов с хроническими заболеваниями, изучая историю болезни и отправляя напоминания пациентам (Yang, Garcia et al., 2024); для этого необходимо выработать рекомендации по лечению с учетом показателей здоровья. Этот тип агентной системы искусственного интеллекта сможет управлять индивидуальным уходом за пациентами и отслеживать ранние признаки ухудшения состояния здоровья, особенно пожилых лиц (Acharya et al., 2025). Еще одна сфера применения агентного ИИ – автоматическое создание нового контента, ориентированного на широкую аудиторию и отвечающего требованиям на основе установленных критериев. Такое приложение было бы полезно для маркетинговых мероприятий, таких как рассылка персонализированных электронных писем покупателям и потенциальным клиентам. Предприниматели и ученые могут осуществлять быстрый поиск литературы с помощью агентного ИИ, что приведет к появлению новых идей. Агентный ИИ может способствовать открытию, разработке и распространению новых лекарств (Gao et al., 2024).

Исследования с помощью агентного ИИ набирают обороты в области науки о морали и принятия этических решений (Small & Lew, 2021). Важность конфиденциальности и безопасности при работе с чувствительной информацией выдвинула этот тип исследований на передний план. Исследования в области морали направлены на то, чтобы создать этическую основу для автономных систем, чтобы агентные системы ИИ могли выбирать действия с учетом их последствий и ценности. В этом контексте интеграция психологии, этики и философии создает общую цель для систем ИИ, которая является этической. Все агентные системы должны соблюдать этические нормы при принятии решений, но в особенности это касается систем здравоохранения и правопорядка, поскольку решения в этих сферах влияют на общество в целом (Acharya et al., 2025).

---

5 Randieri, C. (2025, January 3). Agentic AI: A New Paradigm In Autonomous Artificial Intelligence. Forbes. https://clck.ru/3NedZf

6 Automation Anywhere. (n.d.). What is agentic AI? Key benefits & features. https://clck.ru/3Nedsx

7 Там же.

8 Randieri, C. (2025, January 3). Agentic AI: A New Paradigm In Autonomous Artificial Intelligence. Forbes. https://clck.ru/3NedZf

9 Там же; Automation Anywhere. (n.d.). What is agentic AI? Key benefits & features. https://clck.ru/3Nedsx

Агентные системы искусственного интеллекта требуют самосознания и метапознания (Langdon et al., 2022). Это может быть достигнуто путем создания систем, понимающих свои действия, способности и ограничения, то есть обладающих самореферентными знаниями. Достичь самосознания в системах искусственного интеллекта можно путем самооценки по следующим направлениям: оптимально ли они выполняли задачи; что можно улучшить; какие действия следует предпринять при возникновении сбоев или низкой производительности. Навыки самоуправления при выполнении задачи и способность определять необходимость ее выполнения позволят агентному ИИ оценивать свои стратегии и процессы обучения, чтобы повысить эффективность принятия решений. Новые достижения в исследованиях самосознания и метапознания приведут к созданию более гибких и сложных агентных систем искусственного интеллекта, что, в свою очередь, повысит производительность и надежность работы в мультисредах (Acharya et al., 2025). Это потребует дальнейших исследований в области создания новых моделей ИИ-агентов, адаптивных моральных норм и контекстуального принятия решений (Lai et al., 2021).

2. Практические рекомендации

ИИ-агенты обладают более высокой эффективностью, чем системы с искусственным интеллектом; поэтому они поднимают и более сложные этические и юридические проблемы. Это усугубляется социальной автономией ИИ-агентов. Пользователь, владелец, разработчик имеют определенную степень контроля над пассивными системами искусственного интеллекта (ИИ-ассистентами), поскольку последние привязаны к определенной позиции и предназначены только для решения определенных проблем или задач.

Владельцы, разработчики и пользователи ИИ-агентов обязаны соблюдать этические принципы при проектировании, внедрении и эксплуатации систем. Технический разработчик и владелец алгоритма должны гарантировать, что агентная система искусственного интеллекта применяется этично и законно. Причина этого состоит в том, что агентное программное обеспечение становится независимым после его выпуска; таким образом, необходимо контролировать его действия и проявления. На ком лежит юридическая ответственность, если система искусственного интеллекта выходит из-под контроля? Вред может быть причинен, например, при получении данных от третьей стороны, поскольку система ИИ обладает определенной способностью принимать решения; некоторые считают ее способной на совершение сознательных действий[10] (Lim et al., 2025). Однако пользователь алгоритма агентного ИИ также несет определенную этическую и юридическую ответственность. Что если пользователь попросит ИИ-агента сделать что-то неэтичное и незаконное, например, передать информацию без соблюдения надлежащей правовой процедуры? Кто будет нести ответственность в этой ситуации – пользователь или разработчик/владелец алгоритма ИИ? Что если отношения между ИИ-агентом и пользователем станут нести опасность, а ИИ-агент выйдет из-под контроля и причинит вред (Alberts, Keeling et al., 2024)? Агентный ИИ может контекстуализировать экологический ландшафт, а значит,

[10] Al-Sibai, N. (2022). OpenAI Chief Scientist Says Advanced AI May Already Be Conscious. https://clck.ru/3Nee2Z

обладает осведомленностью; но позволяет ли это пользователю избежать ответственности? Ситуация несет черты сходства с тем, что происходит в области автономных транспортных средств: стороны пытаются снять с себя вину и ответственность.

Выявленные проблемы не настолько распространены среди ИИ-ассистентов. Переход от пассивных технологических систем к интерактивным вызывает дополнительные опасения не только по поводу юридических и этических последствий, но и по поводу масштабов и возможностей агентных систем с искусственным интеллектом. Агентный ИИ – это будущее направление развития искусственного интеллекта, и его не остановить, учитывая множество преимуществ; однако существуют проблемы, которые необходимо признать и решить для защиты общества и человечества. Уважительное отношение к каждому человеку – это отправная точка для того, чтобы сделать агентный ИИ этически и юридически ответственным. Разработка соответствующих структур должна вестись на основе теории базовых психологических потребностей и с учетом особенностей взаимодействия человека и робота (Li et al., 2025; Hosseini & Seilani, 2025; Korzynski et al., 2025; Kshteri, 2025).

Новые приложения агентного ИИ появляются в сфере здравоохранения, логистики и транспорта, а также финансовых услуг. Однако проблемы безопасности и конфиденциальности остаются актуальными из-за увеличения объема данных и роста автономии при принятии решений с помощью агентного ИИ. Такие системы принимают решения, разбивая сложные задачи на отдельные части. Вопрос в том, насколько надежна архитектура принятия решений и насколько хорошо понимается экологическая экосистема, в которой осуществляется процесс принятия решений. Надежность и точность принимаемых решений основываются на этих факторах и зависят от них. Процесс принятия решений и экологическая экосистема являются отправными точками и основополагающими факторами для получения адекватного результата. Если основополагающие аспекты агентного ИИ недостаточно надежны, алгоритм может выйти из-под контроля и начнет ошибаться. Широкий спектр применений агентного ИИ делает необходимым внедрение защитных механизмов на всех уровнях архитектуры, что, в свою очередь, требует иерархической архитектуры систем агентного ИИ. Однако для тестирования подсистем различных архитектур алгоритма потребуется обратная связь, чтобы можно было выделить или исправить те части, которые работают неэффективно или демонстрируют сомнительные результаты. Потребует ли это избыточности в архитектуре агентного ИИ? Если да, то затраты на приобретение и внедрение агентных систем возрастут. Индикатором верного направления развития может стать наличие логики и осознанности, которые, как предполагается, существуют в системах искусственного интеллекта. Коммуникация агентного ИИ клиентам и потенциальным заказчикам с помощью электронной почты сопряжена с различными бизнес-рисками; таким образом, в системе агентного ИИ необходимы защитные механизмы. Проблемы, влияющие на бизнес, могут нанести ущерб репутации бренда и деловым отношениям. Преимущества применения агентного ИИ в новых и перспективных сферах, таких как разработка лекарств, могут привести к тому, что приложение будет работать без необходимых ограничений и без гарантий надежности существующей архитектуры. Перевешивает ли общественная ценность агентного ИИ преимущества обеспечения строгости нормативно-правовой базы? Должна ли защита агентного ИИ, юридическая и нормативная, основываться в большей степени на методе проб и ошибок или на практическом обучении?

Заключение

Сложные ИИ-агенты (агентный ИИ) обладают множеством преимуществ – от способности работать автономно до способности к рассуждениям; следовательно, они обладают определенным уровнем сознания. Однако существуют риски, которые требуют сбалансированного подхода к внедрению агентного ИИ. Сценарии, уже изученные на примере автономных транспортных средств, применимы и к агентному ИИ, а уроки, извлеченные из опыта производства таких автомобилей, являются хорошей отправной точкой для понимания этических и правовых ситуаций в сфере агентного ИИ. Риски, связанные с ИИ, должны быть сбалансированы соответствующими защитными механизмами, которые не должны препятствовать инновациям в применении ИИ. Это требует развития правовой и этической базы для защиты общества, а также для обеспечения преимуществ ИИ в сфере бизнеса и промышленности. Агентный ИИ переводит процесс принятия решений с интерфейса «человек – машина» на взаимодействие «машина – машина» без необходимости вмешательства человека в принятие решений, но нельзя забывать о рисках. Необходимо установить строгие и в то же время гибкие и надежные защитные механизмы для соблюдения этических и правовых рамок.

Список литературы

Abuelsaad, T., Akkil, D., Dey, P., Jagmohan, A., & Vempaty, A. (2024). Agent-E: From Autonomous Web Navigation to Foundational Design Principles in Agentic Systems. *arXiv preprint arXiv:2407.13032*. https://doi.org/10.48550/arXiv.2407.13032

Acharya, D. B., Kuppan, K., & Ashwin, D. B. (2025). Agentic AI: Autonomous intelligence for complex goals – a comprehensive survey. In *IEEE Access (*vol. 13, pp. 18912–18936). https://doi.org/10.1109/ACCESS.2025.3532853

Alberts, L., Keeling, G., & McCroskery, A. (2024). Should agentic conversational AI change how we think about ethics? Characterising an interactional ethics centred on respect. *arXiv:2401.09082v2*. https://doi.org/10.48550/arXiv.2401.09082

Alberts, L., Lyngs, U., & Van Kleek, M. (2024). Computers as Bad Social Actors: Dark Patterns and Anti-Patterns in Interfaces that Act Socially. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–25. https://doi.org/10.1145/3653693

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). Virtual Event Canada: ACM. https://doi.org/10.1145/3442188.3445922

Beulen, E., Plugge, A., & van Hillegersberg. J. (2022). Formal and relational governance of artificial intelligence outsourcing. *Information System E Business Management*, *20*(4), 719–748. https://doi.org/10.1007/s10257-022-00562-7

Coghlan, S., Waycott, J., Lazar, A., & Neves, B. (2021). Dignity, Autonomy, and Style of Company: Dimensions Older Adults Consider for Robot Companions. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1–25. https://doi.org/10.1145/3449178

Gao, S., Fang, A., Huang, Y., Giunchiglia, V., Noori, A., Schwarz, J. R., Ektefaie, Y., Kondic, J., & Zitnik, M. (2024). Empowering biomedical discovery with AI agents. *Cell*, *187*(22), 6125–6151. https://doi.org/10.1016/j.cell.2024.09.022

Grimes, G. M., Schuetzler, R. M., & Giboney, J. S. (2021). Mental models and expectation violations in conversational AI interactions. *Decision Support Systems*, *144*, 113515.

Hasan, S. S., Fury, M. S., Woo, J. J., Kunze, K. N., & Ramkumar, P. N. (2025). Ethical Application of Generative Artificial Intelligence in Medicine. *Arthroscopy: Journal of Arthroscopic Related Surgery*, *41*(4), 874–885. https://doi.org/10.1016/j.arthro.2024.12.011

Hosseini, S., & Seilani, H. (2025). The Role of Agentic AI in Shaping a Smart Future: A Systematic review. *Array*, *26*, 100399. https://doi.org/10.1016/j.array.2025.100399

Kapoor, S., Stroebl, B., Siegel, Z. S., Nadgir, N., & Narayanan, A. (2024). AI Agents That Matter. *arXiv:2407.01502v1*.

Kocielnik, R., Langevin, R., George, J. S., Akenaga, S., Wang, A., Jones, D. P., Argyle, A., Fockele, C., Anderson, L., Hsieh, D. T., Kabir, Y., Duber, H., Hsieh, G., & Hartzler, A. L. (2021). Can I Talk to You about Your Social Needs? Understanding Preference for Conversational User Interface in Health. In *3rd Conference on Conversational User Interfaces (CUI '21), July 27–29, 2021, Bilbao (online), Spain*. ACM, New York, NY, USA. https://doi.org/10.1145/3469595.3469599

Korzynski, P., Edwards, A., Gupta, M. C., Mazurek, G., & Wirtz, J. (2025). Humanoid robotics and agentic AI: reframing management theories and future research directions. *European Management Journa*l, *43*(4), 548–560. https://doi.org/10.1016/j.emj.2025.06.002

Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy*, *49*(6), 102976. https://doi.org/10.1016/j.telpol.2025.102976

Lai, V., Chen, C., Liao, Q. V., Smith-Renner, A., & Tan, C. (2021). Towards a science of human-AI decision making: A survey of empirical studies. *arXiv:2112.11471*. https://doi.org/10.48550/arXiv.2112.11471

Langdon, A., Botvinick, M., Nakahara, H., Tanaka, K., Matsumoto, M., & Kanai, R. (2022). Meta-learning, social cognition and consciousness in brains and machines. *Neural Network*, *145*, 80–89. https://doi.org/10.1016/j.neunet.2021.10.004

Li, X., Shi, W., Zhang, H., Peng, C., Wu, S., & Tong, W. (2025). The Agentic-AI Core: an AI-Empowered, Mission-Oriented core network for Next-Generation mobile telecommunications. *Engineering*. https://doi.org/10.1016/j.eng.2025.06.027

Lim, S., Schmälzle, R., & Bente, G. (2025). Artificial Social Influence via Human-Embodied AI Agent Interaction in Immersive Virtual Reality (VR): Effects of Similarity-Matching during health conversations. *Computers in Human Behavior Artificial Humans*, *5*, 100172. https://doi.org/10.1016/j.chbah.2025.100172

Martinez, D. R., & Kifle, B. M. (2024). *Artificial Intelligence: A Systems Approach from Architecture Principles to Deployment*. MIT Press eBooks, IEEE Xplore2. https://doi.org/10.7551/mitpress/14806.001.0001

Mohanarangan, S., Karthika, D., Moohambigai, B., & Sangeetha, R. (2024). Unleashing the Power of AI and Machine Learning: Integration Strategies for IoT Systems. *International Journal of Scientific Research in Computer Science and Engineering*, *12*(2), 25–32.

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computers are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 72–78). https://doi.org/10.1145/259963.260288

Russell, S. J., & Norvig, P. (1995). *Artificial Intelligence: A Modern Approach*. Prentice Hall. Google-Books-ID: CUVeMwAACAAJ.

Shamsudhin, N., & Jotterand, F. (2021). Social Robots and Dark Patterns: Where Does Persuasion End and Deception Begin? In F. Jotterand, & M. Ienca (Eds.), *Artificial Intelligence in Brain and Mental Health: Philosophical, Ethical & Policy Issues* (pp. 89–110). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-74188-4_7

Shelby, R., Rismani, S., Henne, K., Moon, A., Rostamzadeh, N., Nicholas, P., Yilla, N., Gallegos, J., Smart, A., Garcia, E., & Virk, G. (2023). Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction. *arXiv:2210.05791*. https://doi.org/10.48550/arXiv.2210.05791

Small., C., & Lew, C. (2021). Mindfulness, moral reasoning and responsibility: Towards virtue in ethical decision-making. *Journal of Business Ethics*, *169*(1), 103–117. https://doi.org/10.1007/s10551-019-04272-y

Yang, J., Jimenez, C. E., Wettig, A., Lieret, K., Yao, S., Narasimhan, K., & Press, O. (2024). SWE-AGENT: Agent-Computer Interfaces Enable Automated Software Engineering. *arXiv:2405.15793*. https://doi.org/10.48550/arXiv.2405.15793

Yang, E., Garcia, T., Williams, H., Kumar, B., Ramé, M., Rivera, E., Ma, Y., Amar, J., Catalani, C., & Jia, Y. (2024). From barriers to tactics: A behavioural science-informed agentic workflow for personalized nutrition coaching. *arXiv:2410.14041*. https://doi.org/10.48550/arXiv.2410.14041

Сведения об авторе

Боуэн Гордон– доктор делового администрирования, доцент, школа менеджмента, Университет Англия Рёскин
Адрес: Великобритания, г. Кембридж, CB1 1PT, Ист Роуд
E-mail: gordon.bowen@aru.ac.uk
ORCID ID: https://orcid.org/0009-0007-4082-0336
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56943078600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/65121803
Google Scholar ID: https://scholar.google.com/citations?user=zm_Qgw4AAAAJ

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 10 июня 2025 г.
Дата одобрения после рецензирования – 26 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:340.1:004.8
EDN: https://elibrary.ru/pltfwo
DOI: https://doi.org/10.21202/jdtl.2025.17

Agentic Artificial Intelligence: Legal and Ethical Challenges of Autonomous Systems

Gordon Bowen

Anglia Ruskin University, Cambridge, United Kingdom

Keywords

agentic artificial intelligence,
artificial intelligence,
autonomy,
digital technologies,
ethics,
law,
legal regulation,
liability,
programming,
risk

Abstract

Objective: to identify specific legal and ethical problems of agentic artificial intelligence and develop recommendations for the creation of protective mechanisms to ensure the responsible functioning of autonomous AI systems.

Methods: the research is conceptual in nature and is based on a systematic analysis of scientific literature on the ethics of artificial intelligence, legal regulation of autonomous systems and social interaction of AI agents. The work uses a comparative analysis of various types of AI systems, a study of the potential risks and benefits of agentic artificial intelligence, as well as an interdisciplinary approach that integrates advances in law, ethics, and computer science to form a comprehensive understanding of the issue.

Results: the research has established that agentic artificial intelligence, possessing the decision-making autonomy and ability to social interaction, creates qualitatively new legal and ethical challenges compared to traditional AI assistants. The main categories of potential harm were identified: direct impact on users through overt and covert actions, manipulative influence on behavior, and cumulative harm from prolonged interaction. The author stipulates the need for distributing responsibility between three key actors: the user, the developer and the owner of the agentic artificial intelligence system.

Scientific novelty: for the first time, the research presents a systematic analysis of the ethical aspects of agentic artificial intelligence as a qualitatively new class of autonomous systems that differ from traditional AI assistants in the degree of independence and social interactivity. The author developed a typology of potential risks of social interaction with agent-based intelligent systems and proposes a conceptual model for the distribution of legal and ethical responsibilities in the user-developer-owner triad.

Practical significance: the research forms the theoretical basis for the development of ethical principles and legal norms governing agentic based artificial intelligence in a growing market for autonomous intelligent systems. The findings will be useful for legislators creating a regulatory framework, developers designing protective mechanisms, as well as organizations implementing agentic artificial intelligence systems in various economic fields.

For citation

Bowen, G. (2025). Agentic Artificial Intelligence: Legal and Ethical Challenges of Autonomous Systems. *Journal of Digital Technologies and Law, 3*(3), 431–445. https://doi.org/10.21202/jdtl.2025.17

References

Abuelsaad, T., Akkil, D., Dey, P., Jagmohan, A., & Vempaty, A. (2024). Agent-E: From Autonomous Web Navigation to Foundational Design Principles in Agentic Systems. *arXiv preprint arXiv:2407.13032*. https://doi.org/10.48550/arXiv.2407.13032

Acharya, D. B., Kuppan, K., & Ashwin, D. B. (2025). Agentic AI: Autonomous intelligence for complex goals – a comprehensive survey. In *IEEE Access (*vol. 13, pp. 18912-18936). https://doi.org/10.1109/ACCESS.2025.3532853

Alberts, L., Keeling, G., & McCroskery, A. (2024). Should agentic conversational AI change how we think about ethics? Characterising an interactional ethics centred on respect. *arXiv:2401.09082v2*. https://doi.org/10.48550/arXiv.2401.09082

Alberts, L., Lyngs, U., & Van Kleek, M. (2024). Computers as Bad Social Actors: Dark Patterns and Anti-Patterns in Interfaces that Act Socially. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 1–25. https://doi.org/10.1145/3653693

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 610–623). Virtual Event Canada: ACM. https://doi.org/10.1145/3442188.3445922

Beulen, E., Plugge, A., & van Hillegersberg. J. (2022). Formal and relational governance of artificial intelligence outsourcing. *Information System E Business Management*, *20*(4), 719–748. https://doi.org/10.1007/s10257-022-00562-7

Coghlan, S., Waycott, J., Lazar, A., & Neves, B. (2021). Dignity, Autonomy, and Style of Company: Dimensions Older Adults Consider for Robot Companions. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1–25. https://doi.org/10.1145/3449178

Gao, S., Fang, A., Huang, Y., Giunchiglia, V., Noori, A., Schwarz, J. R., Ektefaie, Y., Kondic, J., & Zitnik, M. (2024). Empowering biomedical discovery with AI agents. *Cell*, *187*(22), 6125–6151. https://doi.org/10.1016/j.cell.2024.09.022

Grimes, G. M., Schuetzler, R. M., & Giboney, J. S. (2021). Mental models and expectation violations in conversational AI interactions. *Decision Support Systems*, *144*, 113515.

Hasan, S. S., Fury, M. S., Woo, J. J., Kunze, K. N., & Ramkumar, P. N. (2025). Ethical Application of Generative Artificial Intelligence in Medicine. *Arthroscopy: Journal of Arthroscopic Related Surgery*, *41*(4), 874–885. https://doi.org/10.1016/j.arthro.2024.12.011

Hosseini, S., & Seilani, H. (2025). The Role of Agentic AI in Shaping a Smart Future: A Systematic review. *Array*, *26*, 100399. https://doi.org/10.1016/j.array.2025.100399

Kapoor, S., Stroebl, B., Siegel, Z. S., Nadgir, N., & Narayanan, A. (2024). AI Agents That Matter. *arXiv:2407.01502v1*.

Kocielnik, R., Langevin, R., George, J. S., Akenaga, S., Wang, A., Jones, D. P., Argyle, A., Fockele, C., Anderson, L., Hsieh, D. T., Kabir, Y., Duber, H., Hsieh, G., & Hartzler, A. L. (2021). Can I Talk to You about Your Social Needs? Understanding Preference for Conversational User Interface in Health. In *3rd Conference on Conversational User Interfaces (CUI '21), July 27–29, 2021, Bilbao (online), Spain*. ACM, New York, NY, USA. https://doi.org/10.1145/3469595.3469599

Korzynski, P., Edwards, A., Gupta, M. C., Mazurek, G., & Wirtz, J. (2025). Humanoid robotics and agentic AI: reframing management theories and future research directions. *European Management Journa*l, *43*(4), 548–560. https://doi.org/10.1016/j.emj.2025.06.002

Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy*, *49*(6), 102976. https://doi.org/10.1016/j.telpol.2025.102976

Lai, V., Chen, C., Liao, Q. V., Smith-Renner, A., & Tan, C. (2021). Towards a science of human-AI decision making: A survey of empirical studies. *arXiv:2112.11471*. https://doi.org/10.48550/arXiv.2112.11471

Langdon, A., Botvinick, M., Nakahara, H., Tanaka, K., Matsumoto, M., & Kanai, R. (2022). Meta-learning, social cognition and consciousness in brains and machines. *Neural Network*, *145*, 80–89. https://doi.org/10.1016/j.neunet.2021.10.004

Li, X., Shi, W., Zhang, H., Peng, C., Wu, S., & Tong, W. (2025). The Agentic-AI Core: an AI-Empowered, Mission-Oriented core network for Next-Generation mobile telecommunications. *Engineering*. https://doi.org/10.1016/j.eng.2025.06.027

Lim, S., Schmälzle, R., & Bente, G. (2025). Artificial Social Influence via Human-Embodied AI Agent Interaction in Immersive Virtual Reality (VR): Effects of Similarity-Matching during health conversations. *Computers in Human Behavior Artificial Humans*, *5*, 100172. https://doi.org/10.1016/j.chbah.2025.100172

Martinez, D. R., & Kifle, B. M. (2024). *Artificial Intelligence: A Systems Approach from Architecture Principles to Deployment*. MIT Press eBooks, IEEE Xplore2. https://doi.org/10.7551/mitpress/14806.001.0001

Mohanarangan, S., Karthika, D., Moohambigai, B., & Sangeetha, R. (2024). Unleashing the Power of AI and Machine Learning: Integration Strategies for IoT Systems. *International Journal of Scientific Research in Computer Science and Engineering*, *12*(2), 25–32.

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computers are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 72–78). https://doi.org/10.1145/259963.260288

Russell, S. J., & Norvig, P. (1995). *Artificial Intelligence: A Modern Approach*. Prentice Hall. Google-Books-ID: CUVeMwAACAAJ.

Shamsudhin, N., & Jotterand, F. (2021). Social Robots and Dark Patterns: Where Does Persuasion End and Deception Begin? In F. Jotterand, & M. Ienca (Eds.), *Artificial Intelligence in Brain and Mental Health: Philosophical, Ethical & Policy Issues* (pp. 89–110). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-74188-4_7

Shelby, R., Rismani, S., Henne, K., Moon, A., Rostamzadeh, N., Nicholas, P., Yilla, N., Gallegos, J., Smart, A., Garcia, E., & Virk, G. (2023). Sociotechnical Harms of Algorithmic Systems: Scoping a Taxonomy for Harm Reduction. *arXiv:2210.05791*. https://doi.org/10.48550/arXiv.2210.05791

Small., C., & Lew, C. (2021). Mindfulness, moral reasoning and responsibility: Towards virtue in ethical decision-making. *Journal of Business Ethics*, *169*(1), 103–117. https://doi.org/10.1007/s10551-019-04272-y

Yang, J., Jimenez, C. E., Wettig, A., Lieret, K., Yao, S., Narasimhan, K., & Press, O. (2024). SWE-AGENT: Agent-Computer Interfaces Enable Automated Software Engineering. *arXiv:2405.15793*. https://doi.org/10.48550/arXiv.2405.15793

Yang, E., Garcia, T., Williams, H., Kumar, B., Ramé, M., Rivera, E., Ma, Y., Amar, J., Catalani, C., & Jia, Y. (2024). From barriers to tactics: A behavioural science-informed agentic workflow for personalized nutrition coaching. *arXiv:2410.14041*. https://doi.org/10.48550/arXiv.2410.14041

Author information

Gordon Bowen – DBA, Associate Professor, School of Management, Anglia Ruskin University
Address: East Road, CB1 1PT, Cambridge, United Kingdom
E-mail: gordon.bowen@aru.ac.uk
ORCID ID: https://orcid.org/0009-0007-4082-0336
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56943078600
WoS Researcher ID: https://www.webofscience.com/wos/author/record/65121803
Google Scholar ID: https://scholar.google.com/citations?user=zm_Qgw4AAAAJ

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 – June 10, 2025
Date of approval – June 26, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:346.6:004.8
EDN: https://elibrary.ru/ruzmxp
DOI: https://doi.org/10.21202/jdtl.2025.18

Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта

Дмитрий Александрович Казанцев

Торгово-промышленная палата Российской Федерации, Москва, Россия

Ключевые слова

автономность,
деликтоспособность,
законодательство,
искусственный интеллект,
нейронная сеть,
право,
рискориентированный подход,
робот,
цифровые технологии,
юридическая ответственность

Аннотация

Цель: формулировка предложений по формированию системы субсидиарной ответственности субъектов за вред, ставший результатом использования систем искусственного интеллекта.

Методы: исследование базируется на комплексной методологической основе, включающей применение абстрактно-логического метода для теоретического осмысления правовой природы искусственного интеллекта как объекта правового регулирования, метода сравнения для анализа подходов российского и европейского законодательства к регулированию деликтной ответственности, методов обобщения для систематизации существующих концепций распределения ответственности между субъектами права, а также корреляционного анализа для выявления взаимосвязей между типологией систем искусственного интеллекта и механизмами правовой ответственности за их функционирование.

Результаты: в ходе исследования обобщены и систематизированы современные теоретико-правовые представления и нормативные акты Европейского союза и Российской Федерации о вариантах распределения субсидиарной ответственности за неблагоприятные последствия работы искусственного интеллекта. Определены потенциальные субъекты ответственности и выявлены ключевые факторы, влияющие на распределение ответственности между ними. Разработана многомерная матрица распределения ответственности между субъектами, учитывающая влияние каждого из них на работу конкретной системы искусственного интеллекта и типологизацию самих систем с точки зрения рискориентированного подхода.

Научная новизна: в работе впервые предложена авторская концепция, сочетающая дифференциацию ролей субъектов с точки зрения их реального влияния на результаты работы искусственного интеллекта, дифференциацию самих систем искусственного интеллекта согласно

рискориентированному подходу и соответствующую двум указанным классификациям систему правовых презумпций распределения ответственности. Новизна заключается в создании многомерной матрицы субсидиарной ответственности, которая позволяет учитывать множество факторов при определении субъекта ответственности в каждом конкретном случае причинения вреда системами искусственного интеллекта, что существенно отличается от существующих односторонних подходов к данной проблематике.

Практическая значимость: выводы и предложения исследования могут быть использованы для развития доктрины субсидиарной ответственности в области использования искусственного интеллекта, разработки и модификации норм права, посвященных регулированию искусственного интеллекта. Предложенная многомерная матрица распределения ответственности может служить теоретическим основанием для совершенствования судебной практики по делам о возмещении вреда, причиненного системами искусственного интеллекта, а также для создания эффективного баланса между стимулированием развития ИИ-технологий и обеспечением защиты прав и законных интересов физических и юридических лиц.

Для цитирования

Казанцев, Д. А. (2025). Правовые механизмы распределения ответственности за вред, причиненный системами искусственного интеллекта. *Journal of Digital Technologies and Law*, *3*(3), 446–471. https://doi.org/10.21202/jdtl.2025.18

Содержание

Введение

Все более широкое использование систем искусственного интеллекта как в повседневной жизни, так и в различных отраслях экономики и даже публичного управления делает нейросети и иные варианты так называемого слабого искусственного интеллекта не просто экспериментальным инструментом, но и фактором правовых отношений. Важной и одной из самых социально значимых граней этих отношений являются отношения деликтные – иными словами, обязательства, возникшие вследствие причинения вреда, вызванного использованием искусственного интеллекта. В более же широком дискурсе требуется решение вопроса о возложении и распределении ответственности за неблагоприятные последствия применения ИИ.

Роботизация производств и все более широкое использование технологий искусственного интеллекта в различных аспектах повседневной жизни переводит

из теоретической в практическую плоскость вопрос о правовых последствиях причинения роботом вреда человеку. Отсутствие соответствующего регулирования создает правовой вакуум, который потенциально может создать ситуацию отсутствия ответственности за целую группу правонарушений.

Это, в свою очередь, с неизбежностью повлечет стремление физических и юридических лиц избегать, насколько это возможно, вовлечения в такие правоотношения, в которых потенциальное нарушение их прав и законных интересов не будет иметь никаких последствий. Проще говоря, неурегулированная правовая ответственность ИИ – это один из ключевых факторов депопуляризации повседневного использования цифровых технологий, а значит, и важное препятствие на пути их развития.

Уже сегодня этот вопрос перестал быть теоретико-правовым. Роботизация производств, выполнения работ и сферы услуг демонстрирует, к сожалению, вполне реальные примеры того, как непродуманное использование искусственного интеллекта наносит ущерб не только правам и законным интересам физических или юридических лиц, но и причиняет ущерб здоровью людей, а в отдельных случаях и вовсе приводит к смертельным исходам. Так, роботизация автотранспорта и сервисов доставки, медицинской диагностики и обработки персональных данных, оставаясь безусловным удобством и перспективным методом повышения качества жизни, обратной своей стороной имеет издержки в виде значимых рисков для жизни и здоровья граждан.

На более высоком уровне обобщения справедливо отнесение систем ИИ к угрозам для базовых гражданских прав. «К очевидным опасностям можно отнести: покушения на неприкосновенность частной жизни путем скрытого наблюдения (практике Европейского суда по правам человека уже известен ряд дел о скрытом наблюдении за служащими на рабочем месте); зависимость осуществления конституционных прав от воли других субъектов (например, провайдеров); ненадлежащее обеспечение конфиденциальности при обработке уже оцифрованной персональной информации; появление дополнительных расходов на приобретение технических средств и устройств (например, обязательное использование электронных дневников школьников в многодетных семьях); привязка к электронному адресу для получения служебной или банковской информации и т. д.» (Ковлер, 2022).

Работа в цифровой среде в целом и последствия действий ИИ в частности не могут и не должны оставаться вне правового регулирования. Недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и организациям, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий искусственного интеллекта отнесены к основополагающим принципам развития ИИ как в Российской Федерации[1], так и за ее пределами.

При самом первом приближении практика подталкивает к выбору одного из нескольких простых решений относительно будущего правового регулирования ИИ.

Первое и, казалось бы, самое очевидное решение – это полный запрет на использование любых систем искусственного интеллекта как потенциально опасных для человека. Сегодня эта опасность уже не сугубо умозрительная. Она доказана на

[1] Указ Президента России № 490 от 10.10.2019 (в ред. Указа Президента Российской Федерации № 124 от 15.02.2024). (2024). Гарант. https://clck.ru/3NXX4N

практике. А значит, необходимо устранить из обихода любые подобные системы, дабы исключить эту угрозу для жизни и здоровья людей.

Однако уже сегодня искусственный интеллект является не только фактором риска, но и фактором повышения качества жизни людей и удобства их работы. В информационную эпоху введение запрета на инструмент обработки информации столь же деструктивно, как введение, например, запрета на использование автомобилей или самолетов по мотивам того, что с прискорбной регулярностью происходят дорожные инциденты и авиакатастрофы.

Сам по себе запрет онтологически является отнюдь не ординарным, а крайним, исключительным инструментом правового регулирования. Проще говоря, если можно в области права обойтись без запрета, то лучше обходиться без него. Введение любого запрета есть не что иное, как констатация кризиса общественных отношений в той или иной сфере и несовершенство общественно-правового регулирования.

Это не означает, что запреты совершенно не нужны и каждый из них деструктивен. Важно лишь использовать этот инструмент правового регулирования с большой осторожностью и лишь там, где его отсутствие способно породить объективно большие риски, чем его наличие.

В качестве примера можно привести дифференциацию риск-факторов использования ИИ в документе, известном как Закон ЕС об искусственном интеллекте[2]. По этому закону однозначному запрету подлежат лишь системы ИИ, предназначенные, например, для биометрической идентификации и категоризации людей, выстраивания систем социальных рейтингов и другие подобные технологии, прямо направленные на разрушение базовых прав и свобод человека и гражданина. Все остальные системы ИИ подлежат лишь более или менее жесткому регулированию: от максимальных требований к системам, потенциально способным создать угрозу для жизни и здоровья человека, до отсутствия каких бы то ни было требований к использованию ИИ в компьютерных играх.

Вторая крайность в решении проблемы правового регулирования неблагоприятных последствий применения ИИ – это приравнивание технологий искусственного интеллекта к обстоятельствам непреодолимой силы или наделение их сходным статусом. На первый взгляд, это уместно в силу того, что логика поиска и обработки информации даже слабым ИИ не является прозрачной для человека, а значит, и решения такой системы для человека далеко не всегда прогнозируемы.

Однако отсутствие полного понимания не означает отсутствие возможности влияния. Продолжая аналогию с тем же автомобилем, можно вспомнить, что в XXI в. большинство автолюбителей имеет довольно смутные представления о нюансах устройства своего авто. И тем не менее каждый из них несет прямую ответственность за последствия управления этим механизмом. Точно так же не выходит за пределы человека воздействие на системы ИИ вплоть до корректировки их алгоритмов, с тем чтобы свести к минимуму риск ошибочных решений по результатам обработки больших данных.

На практике любая аналогия между работой ИИ и обстоятельством непреодолимой силы будет означать фактическое отсутствие правовой ответственности

---

2 European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act). EUR-Lex. https://clck.ru/3NXX6n

за последствия его работы. Исключение же самой такой ответственности очевидным образом формирует пространство для злоупотреблений вплоть до использования технологий искусственного интеллекта для совершения преступлений, которые в этом случае остались бы безнаказанными.

И коль скоро ни полный запрет, ни полная безнаказанность ИИ не представляются разумными и возможными, то третий подход подталкивает нас к тому, чтобы, принимая наличие объективных фактов и возможностей причинения вреда системами искусственного интеллекта, включить ИИ в круг субъектов правовой ответственности – по крайней мере, в тех случаях, когда человек объективно не участвовал и не мог участвовать в принятии искусственным интеллектом ошибочного вредоносного решения. И вот этот подход заслуживает более пристального рассмотрения непосредственно с правовой точки зрения.

1. Робот и человек: основы деликтоспособности

Право, по крайней мере в нынешнем его виде, антропоцентрично. Это регуляторная система, созданная людьми для отношений в обществе людей. Развитие права является отражением общественного развития, и эволюция права подчинена эволюции общества и положения индивида в обществе. Даже тогда, когда мы имеем дело с правовой фикцией, возложение ответственности, например, на юридическое лицо на практике означает возникновение неблагоприятных последствий для конкретных физических лиц: руководителя, сотрудников, собственников и т. д.

Разумеется, правовое регулирование охватывает и корпорации, и роботов, и иные программно-аппаратные комплексы, и механизмы. Не ограничиваясь лишь артефактами человеческой цивилизации, правовое регулирование в определенных ситуациях может затрагивать даже животных и растения (в частности, их селекцию, оборот и обращение с ними). Но нечеловеческий субъект не выступает в качестве субъекта правовых конструкций не в силу своей «ограниченности» или «ущербности» в сравнении с человеком, а лишь в силу того, что эти конструкции многие тысячелетия возникали и развивались именно как регулятор сугубо человеческого поведения.

Так, классическим набором элементов правовой ответственности принято называть наличие субъекта, субъективной стороны, объекта и объективной стороны. И если наличие объекта и объективной стороны не устраняется фактом причинения вреда в результате действий ИИ, то наличие двух оставшихся факторов представляется дискуссионным.

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[3]. И хотя в данной Резолюции перспективы правовой субъектности

[3] European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). (2018). Official Journal of the European Union, 252–257. https://clck.ru/3NXXAJ

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»[4].

Таким образом, на нормативном уровне был поставлен вопрос о том, что использование ИИ может создать высокий или даже недопустимый риск для жизни, здоровья, прав и законных интересов людей – однако этот вопрос не получил своего разрешения. Причем для реализации означенного риска вовсе не обязательны злонамеренные действия ИИ. В этом контексте особую актуальность приобретает определение «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»[5].

На сегодня преждевременными представляются разговоры о присвоении искусственному интеллекту статуса правового субъекта. Сложно не согласиться с мнением о том, что «применение цифровых технологий с использованием искусственного интеллекта на современном уровне его развития не означает появления новых общественных отношений, качественно отличающихся от существующих», а «искусственный интеллект не выступает в качестве цифрового субъекта права в отношениях по обороту цифровых прав в информационной системе оператора. Последний, используя в предпринимательстве цифровые технологии, применяет в бизнес-моделях элементы искусственного интеллекта, которые не порождают цифровых правоотношений» (Андреев, 2021). Иными словами, искусственный интеллект, являясь инструментом для реализации традиционных хозяйственных отношений на новом технологическом уровне, не порождает на сегодняшний день принципиально новых правовых отношений.

Этот вывод верен и с онтологической точки зрения. Навыки обработки больших объемов информации, в том числе с использованием технологий самообучения, не создают мышление и сознание, подобное человеческому. Довольно точное и все еще актуальное определение ИИ дано в упомянутом выше Указе Президента: «Комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека»[6]. На сегодня наиболее реалистичной выглядит концепция искусственного интеллекта как программно-аппаратного комплекса, не имеющего с человеческим разумом ничего общего в плане сущности мышления, однако способного при этом решать в совокупности аналогичные по сложности либо более сложные задачи (Bokovnya et al., 2020).

---

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

5 Nevejans, N. (2016). European Civil Law Rules in Robotics: Study. European Union. https://clck.ru/3NXXFs

6 Указ Президента России № 490 от 10.10.2019 (в редакции Указа Президента Российской Федерации от 15.02.2024 № 124). (2024). Гарант. https://clck.ru/3NXXHJ

И коль скоро сходство не означает тождество, то присвоение роботу антропоморфных черт не означает обретения им тождества с человеком. А значит, с точки зрения и достигнутого уровня развития техники, и актуального уровня развития права 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).

Несмотря на стремительное развитие нейросетей и технологий роботизации, все еще остается актуальным вывод о том, что «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). Присвоение ИИ прав человека стало бы лишь сугубо некорректной экстраполяцией свойств человека на ИИ (Duffy & Hopkins, 2013), не учитывающей специфику ни человека, ни искусственного интеллекта.

Максимально упрощая, можно утверждать: на сегодня преждевременным представляется присвоение ИИ статуса правового субъекта. Да, во многих аспектах ИИ качественно превосходит человека как в скорости обработки информации, так и в самом объеме обрабатываемой информации. Но присвоение роботу антропоморфных черт не означает обретения им тождества с человеком. Точно так же присвоение ИИ правового статуса человека стало бы лишь экстраполяцией свойств человека на ИИ, не учитывающей специфику ни человека, ни искусственного интеллекта.

Сам феномен деликтоспособности неразрывно связан с понятием правосубъектности. Проще говоря, лишь субъект права может нести правовую ответственность. Сторона, субъектом права не являющаяся, ответственности в правовом смысле не несет. Однако в ситуации, когда причиной возникновения деликтных обязательств стали действия ИИ, т. е. субъекта, не относящегося к субъектам права, все равно необходимо наличие механизма правовой ответственности. Очевидно, что даже в случае с вредом, причиненным искусственным интеллектом, субъектом правовой ответственности будет именно субъект права. Или несколько таких субъектов.

При этом важно подчеркнуть, что правовой принцип соразмерности требует возложения ответственности именно на тех лиц, действиями которых прямо или косвенно и было обусловлено возникновение деликтных обязательств.

2. Профилактика нарушений в области использования ИИ

Теоретико-правовое осмысление деликтных последствий использования искусственного интеллекта не стоит ограничивать лишь работой с уже свершившимися фактами и распределением ответственности за них. Представляется, что такой подход в самой сути своей недостаточен. Не только возможно, но и прямо необходимо

включить в круг сперва теоретико-правового обоснования, а затем и прикладного регулирования механизмы профилактики, а точнее – минимизации риска причинения вреда искусственным интеллектом.

Для этого в первую очередь необходимо теоретически обосновать, практически апробировать (а где это возможно и необходимо – еще и нормативно закрепить) корректное соотнесение ролей человека и искусственного интеллекта при реализации бизнес-процессов в хозяйственных отношениях. Правовое регулирование, в свою очередь, должно быть адекватно этим основополагающим подходам. И, прежде всего, следует признать недопустимым возложение на ИИ принятия ключевых решений по вопросам, затрагивающим в каких бы то ни было отношениях права и законные интересы физических и юридических лиц. Эти решения должны оставаться исключительной прерогативой человека везде, где это возможно.

Дело здесь не только и не столько в упомянутом выше принципе антропоцентризма права. Точнее, это обстоятельство обусловлено тем, что в круг потенциальных последствий деятельности робота уже не в качестве субъекта, а в качестве объекта вовлекается человек. Например, в случае принятия решения об аварийном отключении мощностей электростанции или об аварийном сбросе воды из водохранилища даже самый продвинутый алгоритм в отсутствие сложных дополнительных настроек будет оценивать сугубо экономические последствия каждого из возможных решений. И вполне может оказаться, что внезапное затопление близлежащего поселка искусственный интеллект сочтет в данной ситуации экономически целесообразным. По другим мотивам, но с той же роковой логикой может быть принято решение о наезде на пешехода или отключении систем жизнеобеспечения. И постулирование на уровне базовых алгоритмов ИИ принципов «робот должен защищать человека» и «робот не может навредить человеку» не способно нивелировать данный риск: слишком часто линейная логика, оторванная от этики, будет подталкивать к тому, чтобы защитить одного человека путем нанесения вреда другому человеку.

Это возвращает нас к понятию субъективной стороны правонарушения. Высококлассная команда разработчиков может создать алгоритм, позволяющий до известной степени включить в механизм принятия решения роботом интересы человека в качестве наиболее высокого приоритета. Но даже она не сможет придать роботу морально-этические свойства человека, имитировать нравственные переживания и психоэмоциональное отношение к совершаемому действию. Уже существующие системы ИИ обладают такими специфическими характеристиками, как непрозрачность принятия решений для человека, автономность, самообучаемость и непредсказуемость в отдельных случаях с точки зрения человеческой логики (Llorca, 2023).

Не нужно забывать: методы мышления человека и методы обработки информации условным искусственным интеллектом качественным образом отличны. Это два разных типа обработки информации, каждый из которых обладает своими достоинствами и недостатками. И даже при наличии схожих целей неуместно переносить на один тип свойства другого. За пределами данной статьи остается дискуссия о возможности наличия у искусственного интеллекта сознания как такового. Но едва ли можно ожидать от искусственного интеллекта сознания именно человеческого типа.

В этих условиях по общему правилу лишь человек – при этом обладающий и надлежащей экспертизой, и развитыми этическими установками, и именно антропоцентричной аксиологией – может принимать в пределах предоставленных ему полномочий решения, затрагивающие ключевые права и законные интересы другого человека. И потому сегодня искусственный интеллект по общему правилу может быть лишь источником данных для эксперта, а не заменой этого эксперта. Более того, не теряет своей актуальности правило: использование ИИ тем целесообразнее, чем меньше потенциальная ошибка ИИ сможет создать угроз для жизни и здоровья физических лиц.

При соблюдении данного правила не требуются принципиально новые правовые конструкции для регулирования ответственности за вред, ставший следствием работы ИИ. Вопросы распределения деликтных обязательств вполне могут решаться с помощью существующих правовых механизмов. При этом высокая автономия ИИ в вопросах принятия решения, пусть даже не ставящая его в число субъектов права, требует продуманного адаптивного учета специфики ИИ при адаптации существующих норм и принципов права. «Традиционные подходы к распределению юридической ответственности требуют существенной адаптации, что предполагает более детальную, многоуровневую структуру, поддерживающую четкие цепочки подотчетности» (Tianran, 2024).

И одно из самых серьезных направлений адаптации – это регулирование вопросов ответственности в тех ситуациях, когда невозможно сохранить за человеком принятие отдельных решений, поскольку автономия ИИ составляет саму суть автоматизации данного процесса.

В качестве понятного примера можно привести роботизированное такси, автопилот морского судна или робота для микрохирургических операций. Технологическая сложность выполняемых ими задач прямо обуславливает экономическую и прикладную целесообразность устранения человека от контроля за этими операциями. Проще говоря, если за рулем находится водитель, то робот в таком такси уже не нужен – а если такси управляет робот, то наличие водителя нивелирует экономические преимущества от роботизации такси. Именно для подобных ситуаций актуальным является формирование новых правовых механизмов регулирования ответственности за действия искусственного интеллекта.

До известной степени в данной ситуации можно предложить аналогию между ответственностью за действие ИИ и ответственностью за действия младенца: и тот и другой не обладают деликтоспособностью, однако имеют высокую автономию и ограниченную предсказуемость своих действий. Историк права и вовсе может предложить обращение к старым, давно забытым правовым моделям. Речь идет, например, о модели взаимоотношений pater famalias и раба в римском праве. При таком подходе «правовое положение ИИ становится тождественным или близким тому, которое было у римских антропоморфных коллективных организаций, либо еще более редуцированным – раба, домочадцев, детей, в том числе filius in potestate tua est» (Афанасьев, 2022). Однако простой принцип «за все действия раба правовую ответственность несет хозяин» невозможно механистически перенести на модель распределения ответственности за последствия действий робота.

Это отнюдь не означает того, что современный искусственный интеллект более сложен в психоэмоциональном аспекте, чем, например, древнеримский гладиатор. Наоборот, при исследовании первопричин того или иного решения искусственного

интеллекта мы можем с большей легкостью выделить по меньшей мере несколько ключевых субъектов, причем каждый из этих субъектов будет являться физическим лицом, юридическим лицом либо группой лиц. «Отношения с использованием искусственного интеллекта – это всегда отношения между субъектами права или по поводу объектов права. В любом случае это отношения, которые на том или ином этапе инициированы, запрограммированы человеком – субъектом права с той или иной степенью ответственности (в том числе в рамках деятельности юридических лиц). Волеизъявление человека на те или иные действия искусственного интеллекта может быть выражено в разной степени: от действий ИИ, находящихся под полным контролем воли человека, до автономных действий ИИ, опять же допускаемых и осознаваемых в своих возможных пределах и последствиях человеком (группой лиц)» (Шахназаров, 2022).

Эта возможность, в свою очередь, может и должна стать основой для выстраивания модели субсидиарной ответственности (Лаптев, 2019) за действия искусственного интеллекта между теми правовыми субъектами, которые могли прямо или косвенно повлиять на такие действия.

3. Многомерная матрица субсидиарной ответственности за работу ИИ

Вопрос о деликтных обязательствах, возникающих в результате деятельности ИИ, уже не первый год затрагивается в теоретико-правовых работах (Bertolini, 2013). Специальные исследования, как правило, содержат выводы о субсидиарной ответственности или о матрице ответственности, на основании которой вопрос о возложении неблагоприятных правовых последствий решается индивидуально в каждом конкретном случае с учетом комплекса фактов (Bokovnya et al., 2020). Речь идет о таких субъектах, как владелец ИИ, пользователь ИИ, разработчик ИИ, а также третьи лица. Именно на балансе прав, обязанностей и ответственности данных субъектов и представляется целесообразным базировать матрицу распределения правовой ответственности за последствия действий ИИ.

Разумеется, мы не можем применить уголовное или административное наказание к самому ИИ. Любая мера ответственности, примененная к ИИ, в любом случае повлечет за собой неблагоприятные последствия для его пользователя: например, административный запрет на работу ИИ в течение определенного срока будет означать издержки не для самого ИИ, а лишь для того субъекта, который использовал данную систему ИИ в своей хозяйственной деятельности. «При рассмотрении ответственности ИИ целесообразно говорить в первую очередь о деликтной ответственности, т. е. меры ответственности должны быть установлены как реакция на вред, который ИИ может причинить или причиняет. При этом речь не всегда идет о линейной ответственности, т. е. ответственности одного лица за вред, который он причинил, а скорее о совмещенной ответственности, т. е. когда, помимо причинителя вреда, к ответственности могут быть призваны и другие субъекты» (Philipp, 2023).

Теоретико-правовое решение вопроса о распределении ответственности за действия ИИ, повлекшие причинение ущерба физическим и/или юридическим лицам, необходимо в качестве базы для регулирования практических аспектов последствий наступления такой ответственности. «Фундаментальной проблемой в сфере ответственности ИИ является фрагментация ответственности. В отличие от традиционных инструментов, которые функционируют под непосредственным контролем

человека, системы ИИ работают автономно на основе алгоритмического принятия решений. В случаях, когда наступает ответственность за качество продукции, производители, как правило, отвечают за конструктивные недостатки, но что происходит, когда система искусственного интеллекта со временем “учится” вредоносным действиям? Некоторые правоведы выступают за строгую ответственность производителей, как в фармацевтической промышленности, в то время как другие предлагают модели совместной ответственности, включающие разработчиков программного обеспечения, операторов и даже конечных пользователей»[7].

Для решения этого вопроса в первую очередь необходимо определить круг правовых субъектов, обладающих деликтоспособностью и имеющих возможность реально возместить вред, причиненный ошибками ИИ. Например, по давно высказанному мнению Р. Линеса и Ф. Люсиверо, ответственность за вред, причиненный ИИ, несет лицо, его программировавшее, либо лицо, ответственное за его эксплуатацию, в установленных законом рамках (Leenes & Lucivero 2014). При этом принцип правовой соразмерности требует наличия причинно-следственной связи между действием (бездействием) таких лиц и наступлением означенного вреда. С этой точки зрения можно выделить следующие группы потенциальных субъектов ответственности:

1. Разработчик ИИ.
2. Владелец ИИ.
3. Пользователь ИИ.
4. Третьи лица.

В этом перечне обозначены именно группы, в рамках каждой из которых можно выделить отдельные подгруппы. Так, например, на практике можно отделить заказчиков ИИ от его непосредственных разработчиков, в кругу третьих лиц можно выделить тех, кто оказывал непосредственное влияние на алгоритмы ИИ, от тех, кто разместил в открытом доступе недостоверные сведения, ставшие причиной ошибочных решений ИИ, и т. д. Но в любом случае если дополнить приведенный выше обобщенный перечень двумя формами вины, то можно получить двухмерную матрицу субсидиарной ответственности за последствия решений ИИ (табл. 1).

Таблица 1. Базовая матрица виновной ответственности за работу ИИ

Субъект ответственности	Умысел	Неосторожность
Разработчик		
Владелец		
Пользователь		
Третьи лица		
Регулирующие органы		

Именно на результатах выяснения наличия и характера вины в каждом конкретном случае и будет складываться субсидиарная ответственность. Такая матрица позволит на практике учитывать множество факторов: например, соблюдались ли пользователем при эксплуатации ИИ инструкции разработчиков, присутствовали ли в данной конкретной модели ИИ какие-либо ограничения и были ли они доведены

[7] Upadhyay, Sh. (2025, March 6). Navigating Liability in Autonomous Robots: Legal and Ethical Challenges in Manufacturing and Military Applications. https://clck.ru/3NXXNJ

до сведения пользователя, прошла ли система ИИ надлежащее обучение (а если нет, то нанесен ли ущерб по вине разработчика или поставщика данных для обучения), в какой степени владелец мог контролировать работу ИИ, а в какой – действия пользователя и т. д.

Так, например, по результатам проведения экспертизы (а при необходимости и следственных действий) может быть доказано то, что неблагоприятные последствия возникли в силу фундаментальных недочетов разработки. «Когда система искусственного интеллекта приобретается встроенной в другие товары (например, в автомобиль), то представляется маловероятным, что подобные договорные исключения (например, между производителем автомобиля и поставщиком программного обеспечения искусственного интеллекта) могут быть успешно переложены на покупателя автомобиля. В то же время интерес представляет идея о возможности установления границ ответственности разработчиков за дефекты создания выпущенных в оборот систем искусственного интеллекта» (Харитонова и др., 2022)[8].

Тезис о границах ответственности подводит нас к вопросу о правовых презумпциях в сфере регулирования ответственности за действия ИИ. Например, можно распределить такие презумпции ответственности между перечисленными выше субъектами: «Основная ответственность лежит на развертывающих организациях и системных операторах, которые осуществляют непосредственный контроль за применением; они должны обеспечить надлежащее функционирование, мониторинг производительности и применение необходимых мер предосторожности, а также тщательное ведение документации. Во вторую очередь, ответственность лежит на разработчиках и производителях систем; она предполагает соблюдение технических стандартов, стандартов безопасности и требований к документации, включая прозрачность процессов принятия решений и аудита. В-третьих, ответственность лежит на надзорных и регулирующих органах, которые должны устанавливать стандарты, проводить регулярные аудиты и поддерживать эффективные механизмы соблюдения мер. Эта многоуровневая структура обеспечивает всестороннюю ответственность при сохранении четких цепочек подотчетности на протяжении всего жизненного цикла системы» (Tianran, 2024).

Дополнив нашу двухмерную матрицу такими презумпциями, мы получаем следующую логику распределения ответственности за действия ИИ (табл. 2).

Таблица 2. Вариант приоритизации ответственности за работу ИИ

Очередность привлечения к ответственности	Вина	
	Умысел	Неосторожность
1. Владелец		
2. Разработчик		
3. Заказчик		
4. Пользователь		
5. Регулирующие и контролирующие органы		
6. Поставщик информации		
7. Третьи лица		

[8] Наумов, В. Б., Чеховская, С. А., Брагинец, А. Ю., Майоров, А. В. (2021). Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения: доклад НИУ ВШЭ. Москва.

При этом «высокая степень автономности ИИ не может служить основанием для уменьшения ответственности разработчиков, производителей. Если разработчик ИИ обладает большей степенью контроля над функционированием системы с ИИ, чем производитель, собственник или пользователь данной системы, это должно увеличивать ответственность разработчика за причинение вреда. Данный принцип может быть представлен в более универсальной интерпретации: степень контроля над функционированием системы ИИ пропорциональна ответственности за причинение вреда»[9].

Без использования презумпций вопрос о распределении ответственности за действия ИИ и в самом деле будет сложно решить в целом ряде случаев. Однако и столь линейное распределение презумпций представляется известным упрощением. Практикующему юристу очевидно, что этой матрицей невозможно охватить все возможные комбинации ответственности, потенциально возникающие при использовании ИИ. За ее пределами остается невиновное возмещение ущерба (как договорное, так и внедоговорное). За ее пределами остается и конструкция источника повышенной опасности.

Да, по общему правилу ч. 2 ст. 1064 Гражданского кодекса РФ лицо, причинившее вред, освобождается от его возмещения, если докажет, что вред причинен не по его вине. Но из этого правила существуют исключения. Одно из них установлено ст. 1079 Гражданского кодекса: лица, владеющие источником повышенной опасности, обязаны возместить причиненный вред вне зависимости от наличия или отсутствия вины в том случае, если вред был нанесен именно этим источником повышенной опасности. Верховный суд РФ поясняет, что источником повышенной опасности следует считать «любую деятельность, осуществление которой создает повышенную вероятность причинения вреда из-за невозможности полного контроля за ней со стороны человека»[10].

Интуитивно под это определение можно подвести и ИИ, ведь он и автономен в своих решениях, и не до конца подконтролен человеку, и способен причинить вред физическим и юридическим лицам. «Источник повышенной опасности может быть признан через следующие критерии: “деятельность”, “действие” и “вредоносность”. Обозначив необходимые для идентификации источника повышенной опасности критерии, необходимо выяснить, подходит ли ИИ под указанные требования. Категории “деятельности” и “действия”, создающих опасность причинения вреда, подтверждаются технически сложным устройством самой технологии ИИ, а также автономностью выбора стратегии выполнения поставленной задачи. Критерий “вредоносности” раскрывается через сферы, в которых может быть использована технология ИИ. Именно так эксплуатация искусственного интеллекта в медицине при определении диагноза или же в беспилотном управлении транспортным средством предполагает возможность причинения вреда окружающим субъектам. Таким образом, можно прийти к выводу о возможности признания искусственного интеллекта источником повышенной опасности»[11].

---

9 Наумов, В. Б., Чеховская, С. А., Брагинец, А. Ю., Майоров, А. В. (2021). Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения: доклад НИУ ВШЭ. Москва.

10 О применении судами гражданского законодательства, регулирующего отношения по обязательствам вследствие причинения вреда жизни или здоровью гражданина: постановление Пленума Верховного Суда РФ № 1 от 26.01.2010, П. 18.

11 Позднякова, М. (2025, 3 апреля). Признание за искусственным интеллектом источника повышенной опасности: реалии и перспективы. Деловой профиль. https://clck.ru/3NXXbo

И в самом деле, «многие системы ИИ (беспилотные транспортные средства, дроны, роботы-хирурги и т. д.) могут квалифицироваться как источники повышенной опасности, а их применение — как деятельность, несущая повышенный риск для окружающих» (Ижаев, Кутейников 2024). Этот тезис является отправной точкой для конкретизации верного, но абстрактного тезиса об индивидуализации решения о распределении субсидиарной ответственности в каждом конкретном случае с учетом комплекса факторов. «Фиксация в законе новых систем ИИ потребует рассмотрения вопроса о признании их источником повышенной опасности» (Антонов, 2020), и владелец искусственного интеллекта в таком контексте предстает владельцем источника повышенной опасности. По умолчанию, ответственность за неблагоприятные последствия деятельности искусственного интеллекта несет его владелец – но лишь до тех пор, пока не доказана вина иных лиц.

Подводя промежуточный итог изложенным выше тезисам и отчасти дополняя их, можно констатировать, что «по критерию возможности применения имеющегося нормативного правового регулирования к случаям вреда, причиненного системами ИИ, возможны следующие подходы:

– Ответственность за вред, причиненный источником повышенной опасности.

– Ответственность за причинение вреда вследствие недостатков (дефектов) продукта.

– Безвиновная ответственность за вред, причиненный чрезвычайно опасной деятельностью.

– Применение по аналогии норм об ответственности за вред, причиненный животными. В частности, между роботами и животными можно обнаружить некоторое сходство. Например, и роботы, и животные могут действовать независимо от своих владельцев, воспринимать окружающую обстановку и осуществлять действия в зависимости от нее.

– Применение по аналогии норм об ответственности за вред, причиненный работниками. Ответственность работодателя за вред, причиненный работником третьим лицам, связана с действиями работника, повлекшими причинение вреда, которые он совершил в пределах выполнения своих рабочих обязанностей.

– Применение по аналогии норм об ответственности за вред, причиненный детьми»[12].

Все эти подходы по-своему верны, однако каждый из них в полной мере может быть применен лишь к отдельным случаям использования ИИ. Ведь и концепция источника повышенной опасности сегодня уже не способна в полной мере охватить практику использования ИИ. «Очевидно, что существуют различные виды систем ИИ: от робота-пылесоса до автономных дронов, используемых в вооружениях. Большое количество примитивных систем ИИ не будет обладать характеристиками, способными нанести какой-либо существенный вред человеку. В связи с этим использование по умолчанию ст. 1079 ГК РФ и приравнивание всех систем ИИ к источникам повышенной опасности представляется спорным. Отчасти можно согласиться с целесообразностью детализации критериев источников повышенной опасности применительно к системам ИИ. При этом необходимо учитывать, что на практике

[12] Наумов, В. Б., Чеховская, С. А., Брагинец, А. Ю., Майоров, А. В. (2021). Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения: доклад НИУ ВШЭ. Москва.

для определения источника повышенной опасности в конкретной ситуации может использоваться так называемый деятельностный подход. Его суть отражена в постановлении Пленума Верховного Суда РФ № 138 от 26.01.2010. В документе указано, что по смыслу ст. 1079 ГК РФ источником повышенной опасности следует признавать любую деятельность, осуществление которой создает повышенную вероятность причинения вреда из-за невозможности полного контроля за ней со стороны человека, а также деятельность по использованию, транспортировке, хранению предметов, веществ и других объектов производственного, хозяйственного или иного назначения, обладающих такими же свойствами. Такая интерпретация дает возможность суду определять в каждом конкретном случае, является ли та или иная система ИИ источником повышенной опасности» (Ижаев, Кутейников, 2024).

Итак, не всякая система ИИ является источником повышенной опасности. А значит, и применение кратко означенных выше презумпций носит субъектно-объектный характер – проще говоря, зависит не только от статуса субъекта правовой ответственности, но и от характера самой системы ИИ как того объекта, за результаты работы которого и предполагается ответственность.

И здесь мы возвращаемся к рискориентированной классификации Закона ЕС об искусственном интеллекте, упомянутой в самом начале статьи. Для реализации рискориентированного подхода этот Закон ЕС выделяет четыре группы систем ИИ, различающихся в зависимости от цели:

1. Категория недопустимого риска: биометрическая идентификация и категоризация людей, система социального рейтинга и т. п.

2. Категория высокого риска: использование ИИ с потенциальной возможностью создания прямой угрозы для жизни и здоровья человека – например, на транспорте или в медицине.

3. Категория ограниченного риска: использование чат-ботов, использование нейросетей для создания информационного контента.

4. Категория минимального риска: видеоигры, вспомогательные программы, рекомендательные системы.

Сама классификация, безусловно, заслуживает дальнейшего развития. Так, в рамках группы высокорисковых систем стоит обособить системы с риском для жизни и здоровья, с одной стороны, и системы с риском для имущественных интересов физических и юридических лиц – с другой. Среди систем ограниченного риска можно выделить системы общего назначения и специализированные. Но в любом случае при распределении субсидиарной ответственности необходимо учитывать не только то воздействие, которое оказывают деликтосопособные субъекты права на работу ИИ, но и характер конкретной системы ИИ.

Так, например, «в случаях, когда вред причинен высокорисковой системой ИИ, целесообразно использовать строгую ответственность разработчиков. Связано это с тем, что такие системы ИИ по своей природе способны оказать значительное негативное воздействие на права и свободы человека, в связи с чем последний должен обладать повышенными гарантиями защиты» (Ижаев, Кутейников, 2024). Реализация этого подхода смещает дискурс с концепции источника повышенной опасности в сторону установления собственной системы презумпций для каждой группы систем ИИ, обособленных согласно рискориентированному принципу.

В результате у нас появляется многомерная матрица, учитывающая по меньшей мере следующие параметры:

1. Роль деликтоспособного правового субъекта в работе ИИ.
2. Форма вины и наличие оснований для невиновной ответственности.
3. Категория системы ИИ с точки зрения рискориентированного подхода.

В такой многомерной матрице мы уже не ограничены категоричными утверждениями о том, что «за ИИ отвечает в первую очередь владелец» или «за ИИ отвечает разработчик, а всех остальных привлекаем к ответственности лишь после того, как будет доказано отсутствие вины разработчика».

Да, подобная многомерная матрица сложна. Но лишь она позволяет не только реализовать баланс прав и обязанностей, но и соблюсти баланс хозяйственных интересов. Ведь если полное отсутствие правового регулирования ответственности может стать тормозом для развития отрасли ИИ, то и избыточное непроработанное регулирование вполне способно создать аналогичные проблемы. Проще говоря, если презюмировать ответственность владельца за действия ИИ, то никто не захочет покупать такие системы. А если по умолчанию привлекать к ответственности разработчиков, то мало кто захочет их разрабатывать.

Сложно не согласиться с тем, что «в свете возможного возложения ответственности на разработчиков необходимо хотя бы на начальных этапах предусмотреть сбалансированную систему иммунитетов для них, добавив обязательное страхование ответственности, а также регистрацию систем ИИ. В случае признания ИИ субъектом возможно установление режима совмещенной ответственности, когда субсидиарную ответственность могут нести и создатель ИИ, и его владелец или иной субъект»[13]. Представляется, что именно в рамках предложенной выше многомерной матрицы такая субсидиарная ответственность может быть реализована наиболее эффективно.

При всей своей сложности именно многомерная матрица позволит не только включить в круг правового регулирования все случаи использования ИИ, но и учесть вариативность, изменчивость и специфичность комбинаций различных алгоритмов. Например, владелец ИИ становится первым кандидатом на субсидиарную ответственность при наступлении вреда вследствие использования «системы ИИ общего назначения, которые характеризуются возможностью решения широкого спектра задач. По общему правилу их следует определять как системы ИИ низкого риска. Однако если в результате «тонкой настройки» они используются в продуктах, обладающих высоким риском, то такие системы также должны признаваться высокорисковыми с соответствующими последствиями при разрешении споров, вытекающих из причинения вреда» (Philipp, 2023). И для высокорисковых систем презумпция ответственности может быть возложена в первую очередь на заказчиков и разработчиков.

Выводы

Право как феномен и правовые институты как его проявления развиваются не в вакууме сугубо теоретических построений, а лишь в контексте развивающейся практики хозяйственных отношений. В этом смысле теоретическое осмысление

[13] Наумов, В. Б., Чеховская, С. А., Брагинец, А. Ю., Майоров, А. В. (2021). Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения: доклад НИУ ВШЭ. Москва.

технических и экономических реалий следует за появлением этих реалий. Но без теоретического осмысления невозможно ни системное осознание, ни профессиональное регулирование новых отношений.

Сегодня в силу уровня развития техники и вовлечения инновационных технологий в хозяйственные отношения вопрос ответственности ИИ имеет уже не только и не столько теоретико-правовое, сколько практическое значение. Роботы уже сегодня могут не только принести пользу, но и причинить вред и физическим, и юридическим лицам. Более того, «использование алгоритмических систем таит в себе особые угрозы для личных и политических прав – для права на неприкосновенность частной жизни, свободы выражения мнений, а также для права на участие в управлении делами государства посредством демократических процедур. Кроме того, в связи с тем, что алгоритмы и основанные на них технологии искусственного интеллекта построены на обработке поступающих из внешней среды сведений, под особой защитой в алгоритмическом обществе должны находиться права субъектов персональных данных» (Пибаев, Симонова, 2020).

Отсутствие специального регулирования создает правовой вакуум, который потенциально означает отсутствие ответственности за целую группу правонарушений. Это, в свою очередь, один из ключевых факторов депопуляризации повседневного использования цифровых технологий, а значит, и важное препятствие на пути их развития. Однако и непродуманное регулирование может стать точно таким же, если не более существенным препятствием на пути повседневного использования ИИ в бытовых и производственных вопросах.

Первым, но важным шагом в сторону практической регуляторики должна стать теоретико-правовая проработка вопросов ответственности за последствия применения ИИ. «До сих пор отсутствует однозначное понимание того, каким образом следует разрешать проблемы возложения внедоговорной гражданско-правовой ответственности за вред, причиненный системами ИИ. С одной стороны, регулирование должно стимулировать развитие индустрии ИИ и не предусматривать чрезмерно обременительные положения для разработчиков и профессиональных эксплуатантов, а с другой – необходимо обеспечить высокий уровень защиты прав человека и общества, поскольку последние в таких спорах будут заведомо слабой стороной. Таким образом, очевидна актуальность поиска оптимальных и адекватных подходов к правовому регулированию юридической ответственности» (Ижаев, Кутейников, 2024).

Сегодня вопрос об ответственности за последствия действий ИИ может быть решен положительно, поскольку 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» (Ивлиев, Егорова, 2022). А значит, уже сегодня представляется реализуемым на практике и принцип «разграничения ответственности организаций-разработчиков и пользователей технологий искусственного интеллекта исходя из характера и степени причиненного вреда»[14].

[14] Указ Президента России № 490 от 10.10.2019 (в редакции Указа Президента Российской Федерации от 15.02.2024 № 124). (2024). Гарант. https://clck.ru/3NXXig

Однако возможность положительного решения вопроса не означает простоты его решения. Прежде всего, необходимо опираться на следующие фундаментальные посылки:

1. И текущий уровень развития права, и текущий уровень развития технологий искусственного интеллекта не позволяют рассматривать робота в качестве субъекта правовых отношений или субъекта правовой ответственности.

2. Невозможность признания деликтоспособности за искусственным интеллектом не означает необходимости признания за ним статуса форс-мажора или невозможности ответственности за последствия действий искусственного интеллекта.

3. Ответственность за последствия действий искусственного интеллекта распределяется между его создателями, его владельцами, его пользователями и иными лицами, вовлеченными в использование робота в той степени, которая влияет на результаты работы искусственного интеллекта.

4. Комбинация ответственности, в том числе субсидиарной, в каждом конкретном случае зависит как от типа самой системы ИИ, так и от того, чьи действия повлияли на принятие ИИ решения, следствием которого явилось возникновение деликтных обязательств.

Например, «пользователь или владелец может быть привлечен к ответственности, если нарушена инструкция применения искусственного интеллекта, в особенности это касается ситуаций, когда до пользователя доводились какие-либо специфические требования по эксплуатации системы. Если мы говорим о пользователе или владельце, то ближе всего к данному виду отношений – модель ответственности за вред, причиненный источником повышенной опасности. Поставщик данных несет ответственность, если вред возник в период, когда система все еще обучалась, либо в случае предоставления некачественных данных. Также следует учитывать, что система искусственного интеллекта может быть снабжена открытым исходным кодом. В таком случае в литературе возникает вопрос о привлечении к ответственности программистов. Также в некоторых случаях, если вред причинен по глубинным проблемам системы искусственного интеллекта, появляется вопрос о привлечении к ответственности дизайнера или изготовителя системы искусственного интеллекта. Поскольку системы искусственного интеллекта часто работают в упомянутой парадигме “черного ящика”, встает вопрос о невозможности в некоторых случаях вообще установить лицо, по чьей воле или по неосторожности причинен вред» (Харитонова и др., 2022)[15].

В этих условиях положительное решение вопроса о субсидиарной ответственности невозможно без применения правовых конструкций, близких (но не обязательно тождественных) концепции источника повышенной опасности. При этом представляется, что такая конструкция, применимая в сфере ответственности за решения ИИ, не должна ограничиваться лишь возможностью невиновного возложения ответственности.

Несколько упрощая, можно предложить систему презумпций ответственности. В рамках этой системы по нисходящей исследуется вопрос о виновности каждого из деликтоспособных правовых субъектов. И лишь в том случае, когда вину установить объективно невозможно, применяется невиновная ответственность.

---

[15] Наумов, В. Б., Чеховская, С. А., Брагинец, А. Ю., Майоров, А. В. (2021). Правовые аспекты использования искусственного интеллекта: актуальные проблемы и возможные решения: доклад НИУ ВШЭ. Москва.

При этом сама иерархия презумпций зависит от категории ИИ с точки зрения рискориентированного подхода. В рамках такого подхода можно выделить, по крайней мере, следующие категории ИИ:

1. Высокорисковые ИИ, способные создать угрозу для жизни и здоровья человека.
2. Высокорисковые ИИ, способные создать угрозу для имущества физических и юридических лиц.
3. Высокорисковые ИИ, способные создать угрозу разглашения персональных данных и иной информации ограниченного доступа.
4. Среднерисковые ИИ, способные создать угрозу для надлежащего совершения хозяйственных операций.
5. Среднерисковые ИИ, способные создать угрозу для производственных процессов и функционирования инфраструктурных объектов.
6. Среднерисковые ИИ общего назначения.
7. Низкорисковые ИИ.

Для каждой из этих категорий выстраивается индивидуальная система презумпций ответственности следующих субъектов:

1. Владелец ИИ.
2. Заказчик ИИ.
3. Разработчик ИИ.
4. Пользователь ИИ.
5. Регулирующие и контролирующие органы.
6. Поставщики информации для ИИ.
7. Третьи лица.

Схематично предложенную многомерную матрицу ответственности за вред, причиненный действиями ИИ, можно представить в виде следующей таблицы, в которой для каждой ячейки в означенной очередности сперва исследуется вопрос о наличии вины в форме умысла либо неосторожности, а затем – вопрос о возможности невиновного возложения ответственности (табл. 3).

Таблица 3. Многомерная матрица ответственности за работу ИИ

Категория системы ИИ	Субъекты ответственности						
	Владелец	Заказчик	Разработчик	Пользователь	Регулирующие органы	Поставщик информации	Третьи лица
Высокорисковые ИИ, способные создать угрозу для жизни и здоровья	3	1	2	6	4	5	7
Высокорисковые ИИ, способные создать угрозу для имущества	3	1	2	4	5	6	7
Высокорисковые ИИ, способные создать угрозу для информации ограниченного доступа	4	1	2	3	6	5	7
Среднерисковые ИИ, способные создать угрозу для хозяйственных операций	1	4	5	2	3	6	7
Среднерисковые ИИ, способные создать угрозу для производственных процессов	1	3	4	2	6	5	7
Среднерисковые ИИ общего назначения	1	4	3	2	5	7	6
Низкорисковые ИИ	4	3	2	1	5	7	6

Таким образом, формальная невозможность возложить наказание или иную меру правовой ответственности на робота уже сегодня отнюдь не препятствует полноценному включению отношений с использованием технологий искусственного интеллекта в сферу правового регулирования, в том числе и в части правовых последствий причинения вреда. Эти инновационные технологии требуют существенного развития правового регулирования, однако сами по себе не создают ни новых правовых институтов, ни принципиально новых правовых конструкций. А значит, при должном подходе к сущностному осмыслению технологической компоненты такое регулирование может быть успешно реализовано в рамках существующей системы права.

Список литературы

Андреев, В. К. (2021). Приобретение и осуществление прав юридического лица с использованием искусственного интеллекта. *Предпринимательское право*, *4*, 11–17. EDN: https://elibrary.ru/nnesjs. DOI: https://doi.org/10.18572/1999-4788-2021-4-11-17

Антонов, А. А. (2020). Искусственный интеллект как источник повышенной опасности. *Юрист*, *7*, 69–74. EDN: https://elibrary.ru/dwhttx. DOI: https://doi.org/10.18572/1812-3929-2020-7-69-74

Афанасьев, С. Ф. (2022). К проблеме материальной и процессуальной правосубъектности искусственного интеллекта. *Вестник гражданского процесса*, *3*, 12–31. EDN: https://elibrary.ru/fjaogm. DOI: https://doi.org/10.24031/2226-0781-2022-12-3-12-31

Дурнева, П. Н. (2019). Искусственный интеллект: анализ с точки зрения классической теории правосубъектности. *Гражданское право*, *5*, 30–35. EDN: https://elibrary.ru/nckitd. DOI: 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. EDN: https://elibrary.ru/anagtu. DOI: https://doi.org/10.12737/jrl.2022.060

Ижаев, О. А., Кутейников, Д. Л. (2024). Системы искусственного интеллекта и внедоговорная гражданско-правовая ответственность: риск-ориентированный подход. *Lex russica*, *77*(6), 23–34. EDN: https://elibrary.ru/xvabso. DOI: https://doi.org/10.17803/1729-5920.2024.211.6.023-034

Ковлер, А. И. (2022). Антропология прав человека в цифровую эпоху (опыт сравнительного анализа). *Журнал российского права*, *12*, 5–29. EDN: https://elibrary.ru/drklnh. DOI: https://doi.org/10.12737/jrl.2022.125

Лаптев, В. А. (2019). Понятие искусственного интеллекта и юридическая ответственность за его работу. Право. *Журнал Высшей школы экономики*, *2*, 79–102. EDN: https://elibrary.ru/gqatho. DOI: https://doi.org/10.17-323/2072-8166.2019.2.79.102

Пибаев, И. А., Симонова, С. В. (2020). Алгоритмы в механизме реализации конституционных прав и свобод: вызовы цифровой эпохи. *Сравнительное конституционное обозрение*, *6*, 31–50. EDN: https://elibrary.ru/zmmnic. DOI: https://doi.org/10.21128/1812-7126-2020-6-31-50

Харитонова, Ю. С., Савина, В. С., Паньини, Ф. (2022). Гражданско-правовая ответственность при разработке и применении систем искусственного интеллекта и робототехники: основные подходы. *Вестник Пермского университета. Юридические науки*, *58*, 683–708. EDN: https://elibrary.ru/ppvmzr. DOI: https://doi.org/10.17072/1995-4190-2021-58-683-708

Чаннов, С. Е. (2022). Робот (система искусственного интеллекта) как субъект (квазисубъект) права. *Актуальные проблемы российского права*, *12*, 94–109. EDN: https://elibrary.ru/memsif. DOI: https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Шахназаров, Б. А. (2022). Правовое регулирование отношений с использованием искусственного интеллекта. *Актуальные проблемы российского права*, *9*, 63–72. EDN: https://elibrary.ru/yownjo. DOI: https://doi.org/10.17803/1994-1471.2022.142.9.063-072

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

Bokovnya, A. Y. et al. (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, *41*, 115–121. https://doi.org/10.36097/rsan.v1i41.1489

Duffy, S. H., & Hopkins, J. P. (2013). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*.

Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, *6*(2), 194–222.

Llorca, D. F. (2023). Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof. *Journal of Artificial Intelligence Research*, *76*, 613–644. https://doi.org/10.48550/arXiv.2211.01817

Philipp, H. (2023). The European AI liability directives — Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, 1–42. https://doi.org/10.1016/j.clsr.2023.105871

Tianran, L. (2024). Research on Legal Responsibility Attribution for Autonomous Systems: An AI Governance Perspective. *Science of Law Journal*, *3*(7), 166–174. https://doi.org/10.23977/law.2024.030722

Сведения об авторе

Казанцев Дмитрий Александрович – кандидат юридических наук, член Совета по развитию закупок, Торгово-промышленная палата Российской Федерации
Адрес: 109012, Россия, г. Москва, ул. Ильинка, 6/1с1
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 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: 10.19.31 / Право на информацию
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 22 мая 2025 г.
Дата одобрения после рецензирования – 4 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:346.6:004.8
EDN: https://elibrary.ru/ruzmxp
DOI: https://doi.org/10.21202/jdtl.2025.18

Legal Mechanisms for Distributing the Responsibility for the Harm Caused by Artificial Intelligence Systems

Dmitriy Aleksandrovich Kazantsev
Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia

Keywords

artificial intelligence,
autonomy,
delictual dispositive capacity,
digital technologies,
law,
legal lliability,
legislation,
neural network,
risk-oriented approach,
robot

Abstract

Objective: to formulate proposals to form a system of subsidiary liability for harm resulting from the use of artificial intelligence systems.

Methods: the research is based on a comprehensive methodological basis, including the abstract logical method for theoretical understanding of the legal nature of artificial intelligence as an object of legal regulation; the method of comparison to analyze the Russian and European legislations on tort liability; generalization to systematize the existing concepts of responsibility distribution between subjects of law; and correlation analysis to identify the relationships between the typology of artificial intelligence systems and the mechanisms of legal responsibility for their functioning.

Results: the study summarizes and systematizes modern theoretical and legal concepts and regulations of the European Union and the Russian Federation on the distribution of subsidiary responsibility for the adverse effects of artificial intelligence. Potential subjects of responsibility were identified, as well as the key factors influencing the distribution of responsibility between them. A multidimensional matrix was developed for responsibility distribution between the subjects, taking into account their impact on the specific artificial intelligence system functioning and the systems typologization under the risk-based approach.

Scientific novelty: for the first time, an original concept is proposed, which combines the differentiation of the subjects' roles in terms of their real impact on the artificial intelligence results; the differentiation of artificial intelligence systems under the risk-based approach; and the system of legal

presumptions of responsibility distribution corresponding to the above two classifications. The novelty lies in the creation of a multidimensional matrix of subsidiary liability, which allows taking into account many factors when determining the subject of responsibility in each specific case of harm caused by artificial intelligence systems, which differs significantly from existing unilateral approaches to this issue.

Practical significance: the research conclusions and suggestions can be used to develop the doctrine of subsidiary responsibility in the field of artificial intelligence use, to develop and modify the legal norms regulating artificial intelligence. The proposed multidimensional matrix of responsibility distribution can serve as a theoretical basis for improving judicial practice in cases of compensation for damage caused by artificial intelligence systems, as well as for creating an effective balance between stimulating the development of AI technologies and ensuring the protection of the rights and legitimate interests of individuals and legal entities.

For citation

Kazantsev, D. A. (2025). Legal Mechanisms for Distributing the Responsibility for the Harm Caused by Artificial Intelligence Systems. *Journal of Digital Technologies and Law, 3*(3), 446–471. https://doi.org/10.21202/jdtl.2025.18

References

Afanasyev, S. F. (2022). On the problem of substantive and procedural legal personality of artificial intelligence. *Vestnik Grazhdanskogo Protsessa*, *3*, 12–31. https://doi.org/10.24031/2226-0781-2022-12-3-12-31

Andreev, V. K. (2021). Acquiring and exercising rights of a legal entity with the use of artificial intelligence. *Predprinimatelskoe Pravo*, *4*, 11–17. https://doi.org/10.18572/1999-4788-2021-4-11-17

Antonov, A. A. (2020). Artificial intelligence as a source of increased danger. *Yurist*, *7*, 69–74. https://doi.org/10.18572/1812-3929-2020-7-69-74

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

Bokovnya, A. Y. et al. (2020). Legal Approaches to Artificial Intelligence Concept and Essence Definition. *Revista San Gregorio*, *41*, 115–121. https://doi.org/10.36097/rsan.v1i41.1489

Channov, S. E. (2022). Robot (artificial intelligence system) as a subject (quasi-subject) of law. *Actual Problems of Russian Law*, *12*, 94–109. https://doi.org/10.17803/1994-1471.2022.145.12.094-109

Duffy, S. H., & Hopkins, J. P. (2013). Sit, Stay, Drive: The Future of Autonomous Car Liability. *SMU Science & Technology Law Review*, *16*.

Durneva, P. N. (2019). Artificial intelligence: an analysis from the standpoint of the classical legal capacity theory. *Grazhdanskoe Pravo*, *5*, 30–35. https://doi.org/10.18572/2070-2140-2019-5-30-33

Ivliev, G. P., & Egorova, M. A. (2022). Legal issues of the legal status of artificial intelligence and products created by artificial intelligence systems. *Zhurnal Rossiyskogo Prava*, *6*, 32–46. https://doi.org/10.12737/jrl.2022.060

Izhaev, O. A., & Kuteynikov, D. L. (2024). Artificial intelligence systems and non-contractual civil liability: a risk-based approach. *Lex russica*, *77*(6), 23–34. https://doi.org/10.17803/1729-5920.2024.211.6.023-034

Kharitonova, Yu. S., Savina, V. S., & Pagnini, F. (2022). Civil liability in the development and application of artificial intelligence and robotic systems: basic approaches. *Vestnik Permskogo Universiteta. Yuridicheskie Nauki*, *58*, 683–708. https://doi.org/10.17072/1995-4190-2021-58-683-708

Kovler, A. I. (2022). Anthropology of human rights in the digital age (experience of comparative legal method). *Zhurnal Rossiyskogo Prava*, *12*, 5–29. https://doi.org/10.12737/jrl.2022.125

Laptev, V. A. (2019). Artificial intelligence and liability for its work. Law. *Journal of the Higher School of Economics*, *2*, 79–102. https://doi.org/10.17-323/2072-8166.2019.2.79.102

Leenes, R., & Lucivero, F. (2014). Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design. *Law, Innovation and Technology*, *6*(2), 194–222.

Llorca, D. F. (2023). Liability Regimes in the Age of AI: a Use-Case Driven Analysis of the Burden of Proof. *Journal of Artificial Intelligence Research*, *76*, 613–644. https://doi.org/10.48550/arXiv.2211.01817

Philipp, H. (2023). The European AI liability directives — Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, *51*, 1–42. https://doi.org/10.1016/j.clsr.2023.105871

Pibaev, I. A., & Simonova, S. V. (2020). Algorithms in the mechanism of implementation of constitutional rights and freedoms: challenges in the digital age. *Sravnitelnoye Konstitutsionnoye Obozreniye*, *6*, 31–50. https://doi.org/10.21128/1812-7126-2020-6-31-50

Shakhnazarov, B. A. (2022). Legal regulation of relations using artificial intelligence. *Actualniye Problemy Rossiyskogo Prava*, *9*, 63–72. https://doi.org/10.17803/1994-1471.2022.142.9.063-072

Tianran, L. (2024). Research on Legal Responsibility Attribution for Autonomous Systems: An AI Governance Perspective. *Science of Law Journal*, *3*(7), 166–174. https://doi.org/10.23977/law.2024.030722

Author information

Dmitriy A. Kazantsev – Cand. Sci. (Law), member of the Council for developing purchases, Chamber of Commerce and Industry of the Russian Federation, Moscow, Russia
Address: 6/1c1 Ilyinka Str., 109012, Moscow, Russia
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 22, 2025
Date of approval – June 4, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:340.1.721:004.8
EDN: https://elibrary.ru/bvlgsu
DOI: https://doi.org/10.21202/jdtl.2025.19

Техноэтические и правовые аспекты киберзапугивания: структурный анализ дисбаланса сил в цифровой среде

Фотиос Спайропулос

Университет Филипс, Никосия, Кипр
Юридическая компания Spyropoulos Law Firm

Ключевые слова

алгоритмическая прозрачность,
искусственный интеллект,
киберзапугивание,
международное сотрудничество,
право,
технологическая грамотность,
цифровая безопасность,
цифровые платформы,
цифровые технологии,
этика

Аннотация

Цель: исследование направлено на концептуализацию понятия киберзапугивания с точки зрения права, техноэтики и анализ дисбаланса сил в цифровом пространстве как основополагающего фактора причинения вреда в Сети.

Методы: в работе применяется концептуально-аналитическая методология, базирующаяся на междисциплинарном анализе теоретических положений права, техноэтики, философии технологий и социальной психологии. Методологический инструментарий дополнен построением оригинальных концептуальных моделей на основе анализа структурных факторов цифрового пространства, разработкой схем причинно-следственных связей и созданием таксономии форм киберзапугивания. Особое внимание уделено компаративному анализу регулятивных подходов различных юрисдикций и выявлению пробелов в существующих правовых нормах.

Результаты: установлено, что киберзапугивание представляет собой сложный многоуровневый феномен, возникающий на пересечении архитектурных особенностей цифровых платформ, асимметрии технологических компетенций между участниками интеракций и системной фрагментированности законодательного регулирования. Выявлены критические пробелы в ключевых международных правовых инструментах, проявляющиеся в отсутствии унифицированных определений киберзапугивания, недостаточной проработке механизмов трансграничного сотрудничества и нерелевантном учете специфики цифровой среды. Проанализированы фундаментальные этические вопросы, связанные с автоматизированной модерацией контента на основе алгоритмов машинного обучения, проблематикой распределения ответственности между платформами, государственными регуляторами и индивидуальными пользователями, а также противоречиями между обеспечением безопасности и сохранением пользовательской автономии. Выделены четыре основных типа дисбаланса сил: технологический, информационный, социальный и институциональный, каждый из которых требует специфических стратегий преодоления.

Научная новизна: впервые предложен комплексный подход к анализу киберзапугивания как структурно обусловленного злоупотребления цифровой властью через призму техноэтики. Разработанные концептуальные модели представляют новые инструменты для понимания распределенной природы ответственности в цифровой экосистеме и формирования этически обоснованных стратегий профилактики. Введена концепция неправомерного использования информации как центрального механизма систематического злоупотребления властью в цифровой среде.

Практическая значимость: результаты исследования адресованы ученым-правоведам, государственным деятелям и разработчикам цифровых платформ, предлагая практические решения в области этического аудита алгоритмов, создания гибридных систем модерации с участием искусственного интеллекта и человека, формирования международных целевых групп и развития, основанных на правах человека принципов цифровой грамотности. Предложения автора направлены на создание более безопасной, подотчетной и инклюзивной цифровой среды для всех участников.

Для цитирования

Спайропулос, Ф. (2025). Техноэтические и правовые аспекты киберзапугивания: структурный анализ дисбаланса сил в цифровой среде. *Journal of Digital Technologies and Law*, *3*(3), 472–496. https://doi.org/10.21202/jdtl.2025.19

Содержание

Введение

Хотя явление киберзапугивания и становится все более распространенным, оно не имеет общепринятого определения как в Европе, так и на международном уровне (Smith et al., 2013). По данным ЮНИСЕФ, киберзапугивание определяется как «травля

с использованием цифровых технологий»[1]. Аналогичным образом, Европейская комиссия описывает это явление как «неоднократное словесное или психологическое преследование, осуществляемое отдельным лицом или группой лиц, использующих цифровые платформы для распространения вредоносного контента, такого как оскорбительные сообщения или непристойные фотографии, с целью ущемить или унизить жертву»[2].

Организация Объединенных Наций определяет киберзапугивание как форму насилия в Сети, характеризующуюся такими свойствами, как дисбаланс сил, анонимность и широкий охват. В отличие от традиционной травли даже одиночное вредоносное действие в Интернете может считаться актом киберзапугивания, поскольку цифровой контент отличается продолжительностью и широким распространением[3]. Это динамическое, еще развивающееся определение отражает уникальные риски, связанные с цифровыми платформами, включая постоянную доступность и возможность тиражирования вредоносных материалов, которые усугубляют уязвимость жертвы (Langos, 2012; Menesini et al., 2012; Slonje & Smith, 2008).

Научные определения часто опираются на традиционную концепцию травли, предложенную в работе Olweus (1993). Они подчеркивают такие свойства, как использование цифровых инструментов, намерение причинить вред и повторяющиеся действия (Englander et al., 2017; Mouzaki, 2010; Juvonen & Gross, 2008). Центральное место в киберзапугивании занимают использование агрессором технологических преимуществ, тогда как у жертвы может не быть средств для самозащиты, а также анонимность и публичность, обеспечиваемые цифровыми платформами (Kowalski, 2018; Smith et al., 2008; Nocentini et al., 2010; Hinduja & Patchin, 2006). Метафорическое определение Li (2007) – «новая бутылка, но старое вино» – говорит о том, что киберзапугивание повторяет традиционную травлю, в то же время используя отличительные черты цифровых технологий.

Искусственный интеллект (далее – ИИ) вносит дополнительные сложности в эту ситуацию, выступая как инструментом борьбы с киберзапугиванием, так и потенциальной проблемой. Системы на базе ИИ все чаще используются для обнаружения вредоносного контента, служат посредниками при взаимодействии и помогают предотвратить распространение оскорбительных материалов. Однако эти системы часто сталкиваются с ограничениями, такими как трудности в понимании контекста, культурных нюансов или в различении вредоносных намерений от сатиры или критики. Кроме того, агрессоры начали использовать инструменты искусственного интеллекта, такие как дипфейки или автоматизированные боты, для усиления вреда, манипулирования контентом или более широкомасштабных атак. Эти разработки подчеркивают необходимость создания надежных, прозрачных и этичных систем искусственного интеллекта для эффективного противодействия киберзапугиванию (Hasan et al., 2023; Raj et al., 2022).

Психологические и социальные последствия киберзапугивания, особенно среди детей и подростков, значительны – от проблем с психическим здоровьем до разрушенных

1 UNICEF, n.d. Cyberbullying: What is it and how to stop it. https://clck.ru/3NQaBe

2 European Commission. (2009). Safer Internet Programme: Protecting children online. https://clck.ru/3NQaRi

3 United Nations. (2016). Ending the Torment: Tackling Bullying from Schoolyard to Cyberspace. https://clck.ru/3NQaWz; United Nations. (2016). Convention on the Rights of the Child: General Comment No. 20 (2016) on the Implementation of the Rights of the Child during Adolescence (CRC/C/GC/20). https://clck.ru/3NQaZ3

отношений (Campbell & Bauman, 2018). Кроме того, опасность этого явления усугубляется за счет таких форм поведения, как несанкционированное распространение откровенных изображений («секстинг») и др. (Katerelos et al., 2011; Chakraborty et al., 2021).

Эффективной борьбе с киберзапугиванием в глобальном масштабе по-прежнему препятствует отсутствие общепринятого определения этого явления. Устранение этого пробела требует комплексных подходов, включающих образовательные кампании, программы повышения цифровой грамотности, ужесточение правовых норм и международное сотрудничество. При разработке мер, направленных на создание более безопасного и справедливого цифрового пространства, важно признать уникальность явления киберзапугивания, в том числе растущую роль искусственного интеллекта в его развитии.

1. Неправомерное использование информации как систематическое злоупотребление властью при киберзапугивании

Отличительной чертой киберзапугивания, представляющего собой систематическое злоупотребление властью, является неправомерное использование информации в цифровой среде. В этих условиях агрессор использует технологические инструменты для манипулирования, контроля и причинения вреда, извлекая выгоду из уникальных возможностей Интернета. В отличие от традиционных форм травли цифровая сфера позволяет преступникам преодолевать физические границы, использовать масштабируемость онлайн-платформ, анонимность и неуничтожимость цифрового контента для усиления своих действий (Courakis, 2005; Lazos, 2001; Furnell, 2006).

Центральное место в этом явлении занимает расширенная модель дисбаланса сил (рис. 1), которая позволяет понять динамику распределения сил при цифровой травле. Модель выделяет ключевые факторы, способствующие причинению вреда, включая способность агрессора манипулировать информацией, использовать анонимность и охватывать широкую аудиторию. Эти элементы не только расширяют возможности агрессора, но и усиливают уязвимость жертв, оказывая устойчивое и всеобъемлющее воздействие.

Ключевым дополнением к этой модели является концепция неправомерного использования информации, которая включает в себя такие действия, как несанкционированный доступ, манипулирование или распространение частного контента. Киберагрессоры часто используют информацию в качестве оружия, чтобы подорвать психологическое благополучие своих жертв и их социальный статус. В качестве примеров можно привести публикацию конфиденциальных фотографий, создание поддельных профилей или распространение клеветнических материалов. Эти действия иллюстрируют, как цифровая среда изменяет традиционную динамику сил, позволяя агрессорам утверждать свое превосходство и избегать ответственности (Spyropoulos, 2011; Katerelos et al., 2011).

Систематическое неправомерное использование информации еще более усугубляется различиями в технических знаниях и знакомстве с технологиями. Агрессоры часто обладают продвинутыми навыками, которые позволяют им использовать цифровые инструменты с большей точностью, в то время как жертвы, особенно если они имеют ограниченную цифровую грамотность, не в состоянии эффективно реагировать. Этот пробел в знаниях усугубляет дисбаланс сил, заставляя жертв чувствовать себя изолированной и бесправной (Vandebosch & Van Cleemput, 2008; Ybarra & Mitchell, 2004a, 2004b).

Эта динамика подтверждается теорией доступности Гибсона (Gibson, 2014), которая объясняет, как цифровые инструменты формируют поведение пользователей. При киберзапугивании такие технологические возможности, как анонимность и масштабируемость вреда, позволяют агрессорам действовать безнаказанно, усиливая психологический и социальный ущерб, наносимый жертвам (Topcu-Uzer & Tanrıkulu, 2018). Например, широкая доступность таких платформ, как социальные сети, позволяет преступникам охватывать более широкую аудиторию, одновременно защищая себя от разоблачения.

На макроуровне этот дисбаланс сил связан с более широкими структурными факторами. Так, доступ к технологическим знаниям часто зависит от социально-экономических различий, что усиливает системное неравенство. Те, кто находятся в привилегированном положении, с большей вероятностью приобретут передовые знания и ресурсы, что позволит им манипулировать информацией как инструментом контроля и доминирования. Эта динамика отражается и в более масштабных явлениях, таких как политическое киберзапугивание, кибертерроризм и информационная война, где контроль над технологиями и данными занимает центральное место в борьбе за влияние (Millard, 2009; Zannis, 2005; Bosworth et al., 1999).

Предлагаемая усовершенствованная модель дисбаланса сил при киберзапугивании подчеркивает взаимосвязь между этими индивидуальными и системными факторами. Она иллюстрирует, как агрессоры используют технологические инструменты и пробелы в знаниях для укрепления своего превосходства, что усложняет задачу противодействия. Модель предусматривает разработку целевых стратегий, направленных на устранение этих дисбалансов как на индивидуальном, так и на структурном уровне (рис. 1).

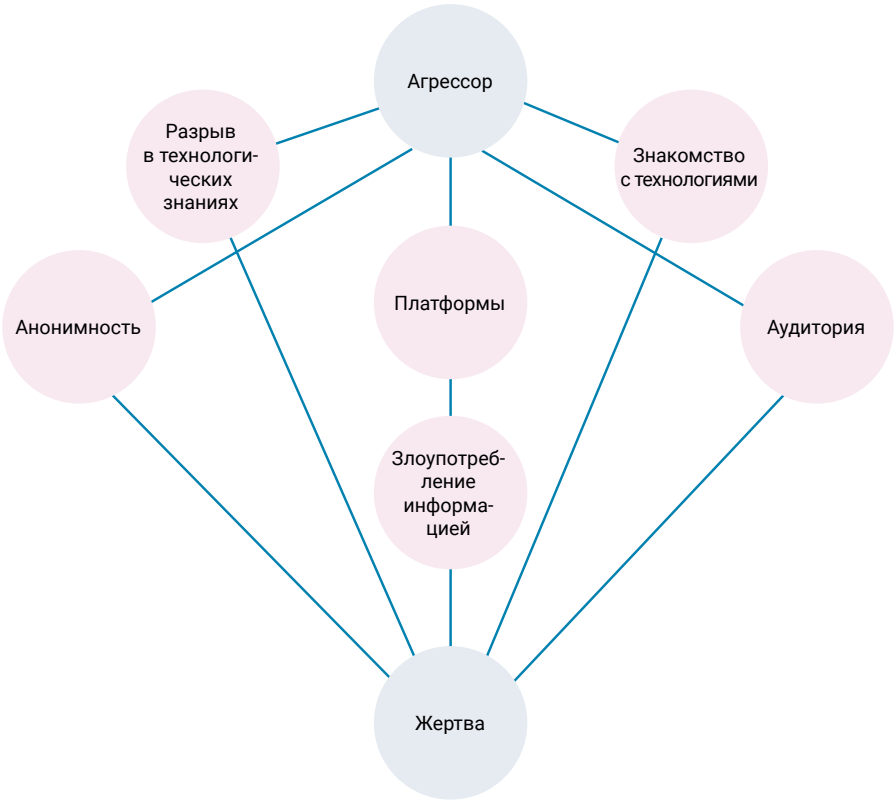

Рис. 1. Усовершенствованная модель дисбаланса сил при киберзапугивании, включающая роль злоупотребления информацией и технологической грамотности в динамике киберзапугивания

Таким образом, систематическое неправомерное использование информации лежит в основе дисбаланса сил, присущего киберзапугиванию. Это явление обусловлено не только поведением отдельных людей, но и технологическими и системными факторами, которые меняют традиционные представления об ущербе и контроле. Решение этой проблемы требует многогранного подхода. Меры противодействия должны быть направлены на устранение пробелов в цифровой грамотности, повышение возможностей граждан к противодействию и укрепление подотчетности платформ. Кроме того, для восстановления баланса сил в цифровой сфере решающее значение имеет обеспечение равного доступа к технологиям и внедрение надежных этических и правовых гарантий. Интегрируя эти стратегии, заинтересованные стороны смогут создать более безопасную, справедливую и инклюзивную цифровую среду.

2. Киберзапугивание и этика в сфере технологий: анализ потоков с точки зрения технологической этики

Киберзапугивание представляет собой не только социотехнический феномен, но и фундаментальную этическую проблему в эпоху цифровых технологий. Как отмечает Luppicini (2018), этика технологий предлагает концепцию, через призму которой можно исследовать взаимосвязь технологий и общечеловеческих ценностей, проливая свет на феномен злоупотребления цифровыми платформами в целях проявления агрессии или причинения вреда. Киберзапугивание, т. е. преднамеренное и повторяющееся вредоносное поведение, осуществляемое с помощью цифровых устройств, усугубляет эти процессы, поскольку агрессоры используют такие возможности, как анонимность, вирусность и непрерывность воздействия на жертву (Langos, 2012; Menesini et al., 2013).

Техноэтические последствия этого феномена разнообразны. Во-первых, киберзапугивание подрывает принцип цифрового достоинства, определяемый как право людей существовать в онлайн-пространстве, не подвергаясь унижению и вредоносному воздействию (Verbeek, 2011). Платформы часто не могут эффективно обеспечить соблюдение этого принципа, хотя и обладают технологическими возможностями для смягчения или выявления вредоносного контента[4]. Это свидетельствует о разрыве между технологическим потенциалом и этической практикой. Как утверждает Moor (2005), новые технологии требуют развития этических норм для предупреждения злоупотребления и развития общественного благосостояния.

Во-вторых, киберзапугивание подчеркивает дисбаланс сил, заложенный в цифровых инфраструктурах. Возможности для причинения вреда распределены неравномерно; агрессоры часто лучше владеют технологиями, в то время как жертвам может не хватать цифровой грамотности или доступа к эффективным механизмам информирования (Spyropoulos, 2011; Katerelos et al., 2011). Эта асимметрия позволяет структурированно распределить техноэтическую ответственность между несколькими участниками, как показано на рис. 2.

[4] Hinduja, S., & Patchin, J. W. (2014). Cyberbullying: Identification, Prevention and Response. Cyberbullying Research Center. https://clck.ru/3NQcNU

Рис. 2. Распределение техноэтической ответственности, показывающее солидарные роли частных лиц, платформ, государства и образовательных учреждений в борьбе с киберзапугиванием

Этот концептуальный инструмент определяет четыре основных уровня ответственности:

1. Ответственность на уровне проектирования. На этом основополагающем уровне находятся системные дизайнеры и разработчики. Они осуществляют выбор архитектуры платформы, функций модерации и доступности, что определяет взаимодействие с пользователями. Если платформа разрешает анонимность без какой-либо системы гарантий или поощряет распространение вредоносного контента без привлечения к ответственности, то вероятность появления киберзапугивания повышается (Capurro, 2009; Tavani, 2011).

2. Ответственность на уровне операторов. Операторы платформы и модераторы контента этически обязаны отслеживать, обнаруживать и удалять вредоносный контент, сохраняя при этом свободу выражения мнений. Неспособность действовать оперативно или прозрачно способствует виктимизации (Zuboff, 2019).

3. Ответственность на уровне пользователей. Этическое поведение – это не только обязанность организаций. Пользователи должны проявлять эмпатию, сдержанность и гражданственность в цифровой среде. Прививать эти техноэтические ценности призваны образовательные программы, ориентированные на молодежь (Chen, 2017; Ortega-Ruiz et al., 2012).

4. Ответственность на законодательном уровне. Такие механизмы, как Общий регламент ЕС по защите персональных данных, обеспечивают прозрачность, подотчетность и соблюдение прав пользователей, воплощая техноэтические нормы в юридических терминах[5]. Более подробно эти механизмы будут рассмотрены в последующих разделах.

[5] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu

Как показывает рис. 2, техноэтическая ответственность за киберзапугивание носит не линейный, а распределенный и взаимозависимый характер. Ни одна из сторон не может решить проблему изолированно. Техноэтический анализ подчеркивает эту взаимосвязь.

Кроме того, новые уровни сложности возникают за счет автоматизации и средств обнаружения на основе искусственного интеллекта. Такие системы предназначены для выявления злоупотреблений, но они также могут создавать предвзятость или упускать нюансы контекста (Ioannou et al., 2018). Поэтому неизменными остаются требования прозрачности и надзора со стороны человека (Tavani, 2011).

Итак, с точки зрения техноэтики явление киберзапугивания показывает необходимость распределения ответственности, разработки этической системы, активного вмешательства и воспитания уважения к цифровому достоинству на всех уровнях социотехнической экосистемы.

3. Взаимосвязь между этикой в сфере технологий, киберзапугиванием и его предотвращением

Техноэтика дает важнейшую основу для изучения этических аспектов киберзапугивания и разработки политики и стратегий по смягчению его последствий. Особо подчеркивая требование совместной ответственности отдельных пользователей, технологических платформ и регулирующих органов, техноэтика выступает за создание более безопасной и справедливой цифровой среды. Предотвращение киберзапугивания и борьба с ним требуют комплексного подхода, выходящего за рамки применения технологических решений или отдельных законодательных мер. Важно отметить, что большинство из этих методов профилактики давно применяются в психологии для развития эмоциональной устойчивости, эмпатии и осознанности поведения. Таким образом, эффективные меры включают в себя этические принципы, образовательные инициативы и инновационные психосоциальные стратегии, обеспечивающие баланс между техническим прогрессом, правами человека и благополучием общества (Hinduja & Patchin, 2009).

Общий регламент по защите данных (GDPR) представляет собой один из самых значимых правовых инструментов для защиты персональных данных в Европейском союзе[6], особенно в контексте причинения вреда в Сети. Документ закрепляет такие принципы, как минимизация объема данных и право на их удаление. Это дает возможность сохранять контроль над своим цифровым присутствием и добиваться возмещения ущерба в случае неправомерного использования личной информации. Общий регламент по защите данных – это не просто механизм регулирования; он воплощает в себе основные техноэтические ценности: прозрачность, подотчетность и автономию, обеспечивая действенную этическую защиту в сфере цифровых прав. Тем самым он способствует созданию более уважительной и ориентированной на человека цифровой среды[7].

---

6 Там же.

7 European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. Official Journal of the European Union, L333, 80–137. https://clck.ru/3QGqvZ

Не менее важен Закон об искусственном интеллекте (AI Act), принятый Европейским союзом в качестве первой глобальной нормы регулирования технологий искусственного интеллекта (Regulation (EU) 2024/1689). Этот закон использует подход к классификации систем искусственного интеллекта с точки зрения категорий риска – от минимального до высокого. Инструменты, используемые для модерации контента и выявления вредоносного поведения в Сети, такого как киберзапугивание, обычно относятся к категории систем высокого риска, требующих строгого соблюдения требований прозрачности, справедливости и надзора. Это гарантирует, что системы искусственного интеллекта, используемые на платформах социальных сетей или в образовательных учреждениях, являются точными, беспристрастными и контролируются операторами-людьми. Кроме того, Закон об искусственном интеллекте запрещает манипулятивные технологии, которые могут пагубно влиять на поведение пользователей. Это отражает принципы приверженности защите прав пользователей и развития этических инноваций.

Конвенция Организации Объединенных Наций против киберпреступности, принятая в 2024 г., представляет собой важную глобальную веху в борьбе с преступлениями, совершаемыми с помощью ИКТ. Она обеспечивает всеобъемлющую основу для борьбы с киберпреступностью, включая незаконный доступ к системам, утечку данных и онлайн-мошенничество. При этом в ней не содержится положений непосредственно о киберзапугивании. Это подчеркивает, что сохраняются трудности в выработке единого глобального подхода к решению этой широко распространенной проблемы. Несмотря на этот пробел, несколько положений конвенции имеют косвенное отношение к киберзапугиванию. Например, ст. 14 касается сексуального насилия над детьми в Интернете, а ст. 16 направлена против несанкционированного распространения изображений интимного характера, что часто связано с киберзапугиванием. Кроме того, ст. 18 устанавливает ответственность платформ, способствующих вредоносной деятельности, а ст. 34 предусматривает меры по оказанию помощи жертвам и их защите[8].

Отсутствие прямых положений о киберзапугивании в Конвенции Организации Объединенных Наций против киберпреступности[9] подчеркивает необходимость принятия дальнейших поправок или дополнительных протоколов. Для устранения этого пробела необходима согласованная международная система борьбы с киберзапугиванием, особенно учитывая транснациональный характер многих инцидентов в этой сфере. Жертвы киберзапугивания часто сталкиваются со значительными препятствиями на пути к правосудию, если преступники действуют в разных юрисдикциях. Разработка универсального определения киберзапугивания заложила бы основу для скоординированных усилий, обеспечив более четкие пути для подачи судебных исков и оказания помощи жертвам. Кроме того, приведение Конвенции в соответствие с техноэтическими принципами повысило бы ее применимость, поскольку это гарантировало бы, что регулирующие меры отражают этические императивы справедливости, подотчетности и защиты пользователей.

---

8 United Nations General Assembly. (2024). United Nations Convention against Cybercrime: Strengthening international cooperation for combating crimes committed via ICT systems and evidence sharing. https://clck.ru/3NQc2k

9 Там же.

Несмотря на эти ограничения, Конвенция служит важным шагом на пути к глобальному сотрудничеству в борьбе с киберпреступлениями. Ее акцент на трансграничное сотрудничество и разделение ответственности государств-членов создает основу, которая может быть адаптирована для решения специфических проблем при киберзапугивании. Поскольку цифровые платформы непрерывно развиваются, в будущие редакции Конвенции необходимо включить положения, непосредственно касающиеся киберзапугивания, что повысило бы актуальность и эффективность документа.

Интегрируя техноэтические принципы в такие инновационные нормативные документы, как Общий регламент по защите данных, Закон об искусственном интеллекте и Конвенция Организации Объединенных Наций против киберпреступности (United Nations General Assembly, 2024), заинтересованные стороны могут создать цифровую экосистему, в которой приоритетными являются безопасность, подотчетность и инклюзивность. Для разработки согласованных стратегий, отвечающих этическим требованиям, важное значение имеет сотрудничество между правительствами, платформами и структурами гражданского общества. Например, партнерские отношения между исследовательскими организациями и государственными органами способствуют разработке передовых инструментов для выявления и смягчения ущерба. Кроме того, этичную и эффективную работу платформ обеспечивает продвижение передовых практик, таких как подотчетность, прозрачность и аудит алгоритмов.

4. Практические и междисциплинарные рекомендации

4.1. Технологические средства

Роль технологий в предотвращении киберзапугивания и борьбе с ним становится все более значимой, поскольку современные платформы внедряют инновационные решения для борьбы с вредоносными действиями в Интернете. Для обнаружения и удаления вредоносного контента крупные платформы используют передовые инструменты искусственного интеллекта. Согласно Meier с соавт. (2016), системы искусственного интеллекта особенно эффективны при мониторинге в режиме реального времени, выявлении подозрительного поведения и предотвращении распространения оскорбительных сообщений. Например, автоматизированные системы могут значительно снизить поток оскорбительных комментариев, своевременно удаляя вредоносный контент.

Однако, хотя ИИ предлагает мощные инструменты для сдерживания вредоносного контента, он не лишен ограничений. Как отмечал Цукерберг[10], системы ИИ с трудом понимают сложные контексты и культурные нюансы, что делает их менее эффективными в ситуациях, требующих вынесения суждений. Для обеспечения точности и беспристрастности при модерации контента необходим гибридный подход, сочетающий технологию искусственного интеллекта с контролем со стороны человека. Это согласуется с подходом Цукерберга[11] , который состоит в вовлечении пользователей с помощью таких инструментов, как Community Notes. Они позволяют

[10] Zuckerberg*, M. (2024). It's time to get back to our roots around free expression. Facebook Watch. https://clck.ru/3NQcAk (* Является соучредителем компании Meta, запрещенной на территории РФ, находящейся в списке экстремистских организаций).

[11] Является соучредителем компании Meta, запрещенной на территории РФ, находящейся в списке экстремистских организаций.

пользователям корректировать контекст и совместно устранять фейковую информацию или вредоносный контент.

С точки зрения техноэтики использование технологий наблюдения и мониторинга в борьбе с киберзапугиванием должно обеспечивать баланс между безопасностью и конфиденциальностью. Floridi (2014) утверждает, что жизненно важное значение для предотвращения практик притеснения имеют прозрачность, уважение прав личности и надежная защита данных. Этичное использование технологий требует наличия систем, которые уделяют приоритетное внимание человеческому достоинству и в то же время предоставляют эффективные решения для снижения вреда, наносимого в Сети.

Помимо совершенствования технологических инструментов, первостепенное значение имеет сотрудничество с участием множества заинтересованных сторон. Государство, гражданское общество и технологические платформы должны совместно разрабатывать протоколы модерации контента для обеспечения баланса между эффективностью и справедливостью. Такое сотрудничество должно быть направлено на создание прозрачных систем, в которых приоритетное внимание уделяется предотвращению вреда и защите прав пользователей. Объединяя опыт и ресурсы, заинтересованные стороны могут разрабатывать решения, характеризующиеся адаптивностью и учетом культурных особенностей. Это позволит преодолеть проблему киберзапугивания в различных цифровых средах.

Дальнейшее повышение эффективности стратегий профилактики возможно путем партнерских отношений с образовательными учреждениями. Школы и университеты могут обучать принципам цифровой этики и мерам противодействия, а также навыкам, необходимым для безопасного и ответственного использования цифрового пространства. Такие программы должны делать упор на критическое мышление, эмпатию и цифровую грамотность, способствуя формированию культуры уважения и подотчетности среди молодого поколения. Совместные инициативы педагогов, государственных органов и платформ должны создать всеобъемлющие образовательные подходы, которые устранят коренные причины киберзапугивания и одновременно будут способствовать этичному цифровому поведению.

Эффективно решить сложные проблемы киберзапугивания возможно, лишь сочетая технологические инновации с этическими принципами и междисциплинарным сотрудничеством. Такой подход способен не только уменьшить ущерб, но и поддержать более общие принципы справедливости, подотчетности и уважения человеческого достоинства, обеспечивая соответствие технического прогресса общественным ценностям.

4.2. Цифровое гражданство и стимулирование ответственного поведения

Техноэтика подчеркивает жизненно важное значение воспитания цифровой гражданственности, выступая за формирование ответственного и уважительного поведения при онлайн-взаимодействиях. Воспитание гражданственности в цифровом мире включает в себя такие важные принципы, как демонстрация уважения к другим, поддержание чувства ответственности в виртуальной среде и воздержание от вредоносного поведения, включая киберзапугивание. Продвижение этих ценностей является неотъемлемой частью предотвращения неправомерных действий в Интернете.

Оно укрепляет социальную ответственность и способствует формированию культуры уважения в цифровой и образовательной среде в целом[12].

4.3. Защита пострадавших

Эффективная защита жертв киберзапугивания требует создания структурированных систем отчетности, ориентированных на их интересы. Такие системы должны обеспечивать надежное и конфиденциальное информирование об инцидентах, при этом гарантируя, что жертвы будут чувствовать себя в безопасности, получать поддержку и расширять свои возможности на протяжении всего процесса. Решающее значение для эффективного рассмотрения жалоб имеют прозрачность и доверие, создавая среду, в которой люди могут с уверенностью обратиться за помощью. С точки зрения техноэтики технологические инструменты должны обеспечивать приоритетность благополучия пострадавших, интегрируя функции, повышающие безопасность и предлагающие доступные способы информирования и поддержки.

Для достижения этих целей необходимы конфиденциальные и безопасные каналы информирования. Ключевую роль в этом могут сыграть образовательные учреждения и коммуникационные платформы, внедрив системы, позволяющие учащимся и пользователям сообщать о травле или домогательствах, не опасаясь мести или нападения. Такие каналы информирования должны быть спроектированы таким образом, чтобы гарантировать анонимность и защиту пользователей, обеспечивая при этом быстрое и эффективное разрешение споров. Например, в работе Ioannou с соавторами (2018) подчеркивается важность интеграции таких инструментов в школьные социальные сети и цифровые платформы. Это укрепит этические подходы как в образовательной, так и в онлайн-среде.

В дополнение к этим механизмам правительствам следует рассмотреть возможность финансирования специальных горячих линий по борьбе с киберзапугиванием. Это может обеспечить пострадавшим немедленный доступ к психологической поддержке и консультациям со стороны подготовленных специалистов, предлагающих советы и помощь с учетом их потребностей. Такие инициативы могут устранить серьезные пробелы в деле помощи пострадавшим, особенно в тех случаях, когда они не имеют доступа к другим ресурсам. Работая с психологическими и эмоциональными аспектами киберзапугивания, такие горячие линии способствуют комплексной защите пострадавших и укреплению психического благополучия.

В дополнение к мерам реагирования можно использовать упреждающий подход к защите пострадавших путем разработки индекса цифровой устойчивости. Этот инструмент позволит оценить способность уязвимых групп, таких как дети и подростки, безопасно и эффективно справляться с киберрисками. Он может оценивать такие факторы, как цифровая грамотность, эмоциональная устойчивость и доступ к системам поддержки, позволяя получить ценную информацию о конкретных потребностях групп риска. Индекс цифровой устойчивости может помочь определить проблемные области и послужить руководством для разработки целевых мер в области образования, повышения осведомленности и при корректировании государственной политики.

---

[12] Bynum, T. W. (2008). Computer and Information Ethics. In The Stanford Encyclopedia of Philosophy. https://clck.ru/3NQcEy

Такие стратегии, ориентированные на пострадавших, не только смягчают непосредственные последствия киберзапугивания, но и способствуют формированию культуры эмпатии и поддержки в цифровом и образовательном пространстве. Tavani (2011) подчеркивает, что приоритетность благополучия жертв и воспитание чувства безопасности являются необходимым условием повышения сопротивляемости пострадавших и дают им возможность восстановить контроль в рамках цифрового взаимодействия. Совместные усилия государства, платформ и структур гражданского общества имеют решающее значение для обеспечения эффективности и широкого доступа к этим системам.

Возможная комплексная система защиты жертв включает защищенные каналы отчетности, финансируемые государством службы поддержки и такие инструменты, как индекс цифровой устойчивости. Эти меры, основанные на принципах техноэтики, направлены на решение многогранных проблем киберзапугивания и способствуют созданию более инклюзивной и благоприятной цифровой среды.

4.4. Этические дилеммы

Использование технологий для предотвращения киберзапугивания, хотя и приносит значительные выгоды, ставит сложные этические и юридические дилеммы, требующие тщательного изучения. Одним из ключевых вопросов является защита конфиденциальности, особенно в контексте методов слежения за данными, используемых платформами социальных сетей. Эти методы направлены на выявление подозрительных действий и предотвращение киберзапугивания, но сопряжены с неизбежным риском злоупотребления властью. Сбор и анализ больших массивов данных, часто проводимый без явно выраженного согласия пользователя, может привести к потенциальным нарушениям прав на неприкосновенность частной жизни и личную автономию, которые охраняются такими нормами, как Общий регламент защиты данных. Это поднимает важные вопросы о том, в какой степени конфиденциальность может быть нарушена для обеспечения безопасности в Интернете.

Другая насущная проблема связана с внедрением алгоритмов модерации контента. Хотя эти инструменты предназначены для обнаружения и удаления вредоносного контента, они часто не учитывают нюансов, позволяющих отличить ненавистнические высказывания от правомерных проявлений сарказма или критики. Это может привести к непреднамеренной цензуре, ограничению свободы выражения мнений, то есть права, закрепленного в международных соглашениях, таких как Европейская конвенция по правам человека (ст. 10 ЕКПЧ)[13]. Такой сценарий подрывает демократический обмен идеями и говорит о необходимости гарантий для предотвращения злоупотреблений.

Эти дилеммы подчеркивают важность соблюдения баланса между правами на неприкосновенность частной жизни и свободу выражения мнений и необходимостью защиты безопасности и достоинства пользователей. Техноэтика предлагает основу для решения этих проблем, выступая за повышение прозрачности методов

[13] Council of Europe. (1950). European Convention on Human Rights, Article 10: Freedom of Expression. https://clck.ru/3NQngR

наблюдения и подотчетность при разработке и внедрении алгоритмов модерации контента. Принятие этой основы поможет предотвратить злоупотребления, укрепить доверие к цифровым платформам и обеспечить соблюдение основных прав при технологическом вмешательстве, одновременно повышая безопасность в Интернете.

4.5. Усиление сотрудничества и перспективы на основе использования данных

Транснациональный характер киберзапугивания требует принятия единых и совместных глобальных ответных мер. Из-за своей способности преодолевать национальные границы киберзапугивание бросает вызов традиционным границам юрисдикций и требует гармонизации правовых рамок для обеспечения последовательной защиты жертв во всем мире. Децентрализованная структура Интернета часто позволяет преступникам использовать различия в национальных законах, что делает необходимым международное сотрудничество. Для эффективного решения этих проблем необходим глобальный подход, основанный на общих принципах справедливости, подотчетности и прав человека.

В этом контексте ключевой рекомендацией является создание Международной целевой группы по предотвращению киберзапугивания, которая способствовала бы проведению трансграничных расследований, обмену информацией и поддержке скоординированных усилий правоохранительных органов. Этот орган мог бы устранить пробелы в отношении юрисдикций путем разработки международно признанных протоколов для ведения дел о киберзапугивании и обеспечения привлечения виновных к ответственности независимо от географического местонахождения. Кроме того, это могло бы способствовать приведению национальных правовых рамок в соответствие с международными стандартами, уменьшению фрагментации политических мер и обеспечению справедливой правовой защиты пострадавших.

На уровне государственной политики многообещающие подходы к борьбе с киберзапугиванием демонстрируют несколько национальных инициатив. Государства реализуют различные стратегии, начиная от кампаний по повышению цифровой грамотности и технологических инструментов и заканчивая специализированными правовыми нормами, описывающими специфический вред от агрессии в Сети. Например, в Греции было представлено цифровое приложение «Безопасность для молодых»[14]. Это инновационный инструмент, предназначенный для оказания помощи несовершеннолетним в возрасте от 12 лет в борьбе с онлайн-угрозами. Приложение обеспечивает прямую связь со службами экстренной помощи, незаметные экстренные уведомления об угрозах в режиме реального времени и безопасную систему подачи сообщений о злоупотреблениях через Единый цифровой портал государственного управления. Придавая приоритетное значение доступности, конфиденциальности и оперативности, данная инициатива выражает технo-этический подход к цифровой безопасности, позволяющий несовершеннолетним

[14] Ministry of Citizen Protection, Hellenic Police and Vodafone Foundation. (2024). SAFE.YOUth: Digital Application for the Protection of Minors. https://clck.ru/3NQcsT

безопасно справляться с кризисными ситуациями. Однако серьезной проблемой остается обеспечение равного доступа к этому инструменту, особенно для маргинализированных групп населения или лиц с ограниченной технической грамотностью.

Несмотря на прогресс в реализации таких национальных инициатив, как «Безопасность для молодых», серьезной проблемой в существующих правовых системах является их адаптируемость к возникающим технологическим угрозам. Многие законы сосредоточиваются на традиционных механизмах онлайн-травли, но не учитывают распространение вредоносного контента под управлением алгоритмов, злоупотребление искусственным интеллектом и роль цифровой анонимности в закреплении злоупотреблений. В будущем нормативно-правовая база должна учитывать эту меняющуюся динамику, особенно в отношении алгоритмов социальных сетей, игровых платформ и контента, созданного с помощью искусственного интеллекта (например, дипфейков). Расширение правовой защиты в этих областях имеет решающее значение для целей актуальности и эффективности законодательных мер.

С точки зрения криминологии киберзапугивание отражает дисбаланс сил, т. е. преступники действуют безнаказанно, используя анонимность и широкий охват цифровых платформ. Хотя юридические механизмы привлечения к ответственности предоставляют жертвам средства правовой защиты, необходимы долгосрочные культурные и системные изменения, чтобы устранить более общие социальные механизмы, которые способствуют цифровой агрессии. Более целостный подход к профилактике и борьбе с этим явлением (Vandebosch, 2019) предполагает интеграцию принципов восстановительного правосудия (Guardabassi & Nicolini, 2024; Duncan, 2016), применение программ реабилитации правонарушителей (Othman et al., 2024) и создание надежных систем поддержки пострадавших.

Наряду с правовыми и институциональными мерами реагирования, решающее значение для понимания тенденций киберзапугивания и разработки эффективных мер вмешательства имеет интеграция информации, основанной на реальных данных. Проведение метаанализа распространенности киберзапугивания и изучение факторов риска, связанных с конкретными платформами, помогает в разработке целенаправленных стратегий профилактики (Sathya & Fernandez, 2024; Kim et al., 2021). Например, изучение того, как алгоритмы усиливают вредоносный контент или как анонимность способствует преследованию, дает ценную информацию о снижении негативного воздействия этих технологий (Johora et al., 2024; Meier et al., 2016).

Другой многообещающий способ борьбы с киберзапугиванием состоит в заключении соглашений об анонимном обмене данными между цифровыми платформами и исследовательскими институтами. Платформы социальных сетей собирают огромное количество поведенческих данных, которые, при условии ответственной анонимизации, могут быть использованы для выявления форм злоупотреблений и разработки упреждающих решений. Прозрачные соглашения, соблюдающие баланс между правом на неприкосновенность частной жизни и задачами исследований, могут обеспечить как развитие инноваций, так и защиту отдельных пользователей (Floridi, 2014).

Укрепление международного сотрудничества, совершенствование национальной правовой базы и использование аналитических данных являются условиями для разработки согласованной глобальной стратегии борьбы с киберзапугиванием. Такие инициативы, как «Безопасность для молодых» в Греции, демонстрируют потенциал

цифровых инструментов в борьбе с онлайн-угрозами, но они должны дополняться всеобъемлющими мерами на международном уровне. Интеграция принципов технэтики, которые ставят во главу угла подотчетность, цифровые права и равный доступ к механизмам защиты, имеет ключевое значение для создания более безопасной, инклюзивной и устойчивой цифровой среды для будущих поколений.

Заключение

Киберзапугивание как распространенная форма цифровой агрессии является примером неправомерного использования технологий для причинения вреда, запугивания или унижения людей. Решение этой многогранной проблемы требует целостного подхода, который объединяет меры профилактики, правовые механизмы, технологические инновации и этические соображения. Центральное место в этой работе занимает признание структурного неравенства, например, в отношении доступа к технологиям и грамотности. Эти различия усиливают уязвимость и закрепляют дисбаланс сил при цифровом взаимодействии (Lazos, 2001). Вооружение пользователей знаниями и формирование этической культуры использования информации остаются важнейшими шагами на пути к продвижению ответственного взаимодействия в цифровой среде (Tsouramanis, 2005).

В рекомендациях относительно мер государственной политики особое внимание должно уделяться адаптивным и перспективным правовым рамкам как на национальном, так и на международном уровнях. Правительствам следует налаживать сотрудничество в целях гармонизации законов, направленных на борьбу с киберзапугиванием, обеспечивая согласованность и подотчетность в различных юрисдикциях. Создание Международной целевой группы по предотвращению киберзапугивания, а также Глобального договора о предотвращении киберзапугивания может послужить базой для трансграничных расследований и обеспечить единые стандарты борьбы с этой проблемой. Эти структуры должны быть динамичными и включать такие передовые технологии, как искусственный интеллект, блокчейн и алгоритмическая прозрачность, которые дают возможность как наносить, так и предотвращать ущерб.

Принятие комплексных мер реагирования требует сотрудничества между заинтересованными сторонами. Технологические платформы несут главную ответственность за разработку и внедрение надежных систем модерации контента, механизмов прозрачности и мер защиты пользователей. Правительства должны принять адаптивные законы, обеспечивающие баланс между свободами личности и защитой от вреда в Сети. Организации гражданского общества и образовательные учреждения также играют ключевую роль в формировании этических норм, повышении осведомленности и оказании поддержки пострадавшим.

Краеугольным камнем борьбы с киберзапугиванием остается профилактика. Образовательные учреждения должны включать в учебные планы вопросы цифровой грамотности, повышения сопротивляемости и этичного использования технологий, что позволит учащимся ответственно ориентироваться в онлайн-пространстве. Эта работа должна дополняться информационно-просветительскими кампаниями и инициативами по вовлечению родителей, финансируемыми за счет бюджета. Необходимо формировать культуру эмпатии и ответственности. Кроме того, важно преодолеть цифровой разрыв и обеспечить равный доступ к технологиям. Это имеет

решающее значение для устранения системного неравенства, которое усугубляет киберзапугивание. Обеспечение всех пользователей, особенно уязвимых групп, инструментами и знаниями для безопасного взаимодействия в цифровом пространстве соответствует этическим принципам инклюзивности и социальной справедливости.

При внедрении технологических инструментов, таких как модерация контента с помощью искусственного интеллекта и технологии слежки, сохраняются этические дилеммы сочетания эффективности с уважением к частной жизни и человеческому достоинству. Принципы техноэтики – ответственность, подотчетность и инклюзивность – отвечают целям общественного благополучия и должны лежать в основе этих инноваций.

В заключение отметим, что борьба с киберзапугиванием требует междисциплинарного, основанного на сотрудничестве подхода, который подразумевает инновационные меры государственной политики, участие всех заинтересованных сторон и этическое предвидение. Устраняя первопричины киберзапугивания, содействуя равному доступу к технологиям и воспитывая культуру ответственности, общество может уменьшить вред от этого негативного явления. Тем самым мы сможем гарантировать, что технологические достижения будут способствовать созданию более безопасной и инклюзивной цифровой экосистемы, в которой приоритетными являются права, достоинство и благополучие всех пользователей.

Список литературы

Bosworth, K., Espelage, D. L., & Simon, T. R. (1999). Factors associated with bullying behavior in middle school students. *The Journal of Early Adolescence*, *19*(3), 341–362. https://doi.org/10.1177/0272431699019003003

Chakraborty, S., Bhattacherjee, A., & Onuchowska, A. (2021). Cyberbullying: A review of the literature. SSRN. http://dx.doi.org/10.2139/ssrn.3799920

Campbell, M., & Bauman, S. (2018). Cyberbullying: Definition, consequences, prevalence. In M. Campbell & S. Bauman (Eds.), *Reducing Cyberbullying in Schools* (pp. 3–16). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00001-8

Capurro, R. (2009). Digital ethics. *The Information Society*, *25*(3), 183–186. https://doi.org/10.1080/01972240902848902

Chen, C. W. Y. (2017). "Think before you type": The effectiveness of implementing an anti-cyberbullying project in an EFL classroom. *Pedagogies*, *13*(1), 1–18. https://doi.org/10.1080/1554480X.2017.1363046

Courakis, N. (2005). *Criminological horizons. Vol. II: Pragmatic approach and individual issues*. 2nd ed. Athens – Komotini: Ant. N. Sakkoula (In Greek).

Duncan, S. H. (2016). Cyberbullying and restorative justice. In R. Navarro, S. Yubero & E. Larrañaga (Eds.). *Cyberbullying Across the Globe* (pp. 239–257). Cham: Springer International Publishing.

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining cyberbullying. *Pediatrics*, *140*(Supplement_2), S148–S151. https://doi.org/10.1542/peds.2016-1758u

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Furnell, S. M. (2006). *Computer Insecurity: Risking the System*. Oxford: Chandos Publishing.

Gibson, J. J. (2014). The theory of affordances (originally published 1979). In G. Bridge & S. Watson (Eds.). *The People, Place, and Space Reader* (pp. 56–60). London: Routledge.

Guardabassi, V., & Nicolini, P. (2024). Adolescence and cyberbullying: a restorative approach. In *INTED2024 Proceedings* (pp. 4562–4570). IATED. https://doi.org/10.21125/inted.2024.1183

Hasan, M. T., Hossain, M. A. E., Mukta, M. S. H., Akter, A., Ahmed, M., & Islam, S. (2023). A review on deep-learning-based cyberbullying detection. *Future Internet*, *15*(5), 179. https://doi.org/10.3390/fi15050179

Hinduja, S., & Patchin, J. W. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169. https://doi.org/10.1177/1541204006286288

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.

Ioannou, A., Blackburn, J., Stringhini, G., De Cristofaro, E., Kourtellis, N., & Sirivianos, M. (2018). From risk factors to detection and intervention: a practical proposal for future work on cyberbullying. *Behaviour & Information Technology*, *37*, 258–266. https://doi.org/10.1080/0144929X.2018.1432688

Johora, F. T., Khan, M. S. I., Kanon, E., Rony, M. A. T., Zubair, M., & Sarker, I. H. (2024). A data-driven predictive analysis on cyber security threats with key risk factors. *arXiv preprint arXiv:2404.00068*.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, *78*(9), 496–505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Katerelos, I., Tsekeris, C., Lavdas, M., & Demetriou, K. (2011). A psychosociological approach to Internet use and mass online role-playing games. In K. Siomos & G. Floros (Eds.), *Research, prevention, management of risks in Internet use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Kim, S., Razi, A., Stringhini, G., Wisniewski, P. J. and De Choudhury, M. (2021). A human-centered systematic literature review of cyberbullying detection algorithms. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2). https://doi.org/10.1145/3476066

Kowalski, R. (2018). Cyberbullying. In J. P. Forgas, R. F. Baumeister & T. F. Denson (Eds.), *The Routledge International Handbook of Human Aggression* (pp. 131–142). London: Routledge. https://doi.org/10.4324/9781315618777-11

Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, *15*(6), 285–289. https://doi.org/10.1089/cyber.2011.0588

Lazos, G. (2001). *Information Technology and Crime*. Athens: Nomiki Bibliothiki. (In Greek).

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(4), 1777–1791. https://doi.org/10.1016/j.chb.2005.10.005

Luppicini, R. (2018). *The Changing Scope of Technoethics in Contemporary Society*. Hershey, PA: Information Science Reference. https://doi.org/10.4018/978-1-5225-5094-5

Meier, A., Reinecke, L., & Meltzer, C. E. (2016). "Facebocrastination"? Predictors of using Facebook* for procrastination and its effects on students' well-being. *Computers in Human Behavior*, *64*, 65–76. https://doi.org/10.1016/j.chb.2016.06.011

Menesini, E., Nocentini, A., & Palladino, B. E. (2012). Empowering students against bullying and cyberbullying: Evaluation of an Italian peer-led model. *International Journal of Conflict and Violence*, *6*(2), 313–320. https://doi.org/10.4119/ijcv-2922

Menesini, E., Nocentini, A., & Camodeca, M. (2013). Morality, values, traditional bullying, and cyberbullying in adolescence. *British Journal of Developmental Psychology*, *31*(1), 1–14. https://doi.org/10.1111/j.2044-835X.2011.02066.x

Millard, G. (2009). Stephen Harper and the politics of the bully. *Dalhousie Review*, *89*(3), 329–336.

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, *7*(3), 111–119. https://doi.org/10.1007/s10676-006-0008-0

Mouzaki, D. (2010). International scientific conference on: "Dealing with cyberbullying from a legal perspective". *The Art of Crime*, *15*. (In Greek).

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. *Australian Journal of Guidance & Counselling*, *20*(2), 129–142. https://doi.org/10.1375/ajgc.20.2.129

Olweus, D. (1993). *Bullying at School: What We Know and What We Can Do*. Oxford, UK: Blackwell.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, building and living together on internet and social networks: the ConRed cyberbullying prevention program. *International Journal of Conflict and Violence*, *6*(2), 303–313. https://doi.org/10.4119/ijcv-2921

Othman, S. N., Alziboon, M. F., Dawood, M., Sachet, S. J., & Moroz, I. (2024). New rehabilitation against electronic crimes by young people. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, *22*, 363–385. https://doi.org/10.5281/zenodo.13732745

Raj, M., Singh, S., Solanki, K., & Selvanambi, R. (2022). An application to detect cyberbullying using machine learning and deep learning techniques. *SN Computer Science*, *3*(5), 401. https://doi.org/10.1007/s42979-022-01266-w

Sathya, J., & Fernandez, F. M. H. (2024). Predictive analysis in healthcare systems. In A. J. Anand, K. Kalaiselvi & J. M. Chatterjee (Eds.), *Artificial Intelligence – Based System Models in Healthcare* (pp. 131–152). Wiley. https://doi.org/10.1002/9781394242528.ch6

* Социальная сеть принадлежит Meta, признанной экстремистской организацией, ее деятельность запрещена на территории Российской Федерации.

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, *49*(2), 147–154. https://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Smith, P. K., del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology* (pp. 26–40). New York: Routledge/Taylor & Francis Group.

Spyropoulos, F. (2011). The manifestations of deviant behavior on the Internet – Reflections on the needs of modernization of Greek criminal legislation. In K. Siomos & G. Floros (Eds.), *Research, Prevention, Management of Risks in Internet Use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Tavani, H. T. (2011). *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing* (3rd ed). Hoboken, NJ: Wiley.

Topcu-Uzer, C., & Tanrıkulu, İ. (2018). Technological solutions for cyberbullying. In M. Campbell & S. Bauman (Eds.), *Reducing cyberbullying in schools* (pp. 33–47). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00003-1

Tsouramanis, Ch. (2005). *Digital Crime – The (Un)Safe Side of the Internet*. Athens: V. Katsaros Publications. (In Greek).

Vandebosch, H. (2019). Cyberbullying prevention, detection and intervention. In W. Heirman, M. Walrave & H. Vandebosch (Eds.), *Narratives in Research and Interventions on Cyberbullying among Young People* (pp. 29–44). Cham: Springer. https://doi.org/10.1007/978-3-030-04960-7_3

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, *11*(4), 499–503. https://doi.org/10.1089/cpb.2007.0042

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226852904.001.0001

Ybarra, M. L., & Mitchell, K. J. (2004a). Online aggressors/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*, 1308–1316. https://doi.org/10.1111/j.1469-7610.2004.00328.x

Ybarra, M. L., & Mitchell, K. J. (2004b). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*, 319–336. https://doi.org/10.1016/j.adolescence.2004.03.007

Zannis, A. (2005). *Cybercrime*. Athens-Komotini: Sakkoulas Publications. (In Greek).

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Сведения об авторе

Спайропулос Фотиос – научный сотрудник, PhD, доцент в области уголовного права и криминалистики, факультет права, Университет Филипс; старший партнер юридической компании Spyropoulos Law Firm
Адрес: Кипр, 28008, г. Никосия, ул. Ламиас, д. 4-6; Греция, 11474, г. Афины, Александрас авеню, д. 81
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.1 / Теоретико-исторические правовые науки

История статьи

Дата поступления – 29 мая 2025 г.
Дата одобрения после рецензирования – 12 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:340.1.721:004.8
EDN: https://elibrary.ru/bvlgsu
DOI: https://doi.org/10.21202/jdtl.2025.19

Techno-Ethical and Legal Aspects of Cyberbullying: Structural Analysis of Power Imbalances in the Digital Sphere

Fotios Spyropoulos

Philips University, Nicosia, Cyprus
Spyropoulos Law Firm, Athens, Greece

Keywords

algorithmic transparency,
artificial intelligence,
cyberbullying,
digital platforms,
digital security,
digital technologies,
ethics,
international cooperation,
law,
technological literacy

Abstract

Objective: to conceptualize cyberbullying from the viewpoint of law and technoethics; to analyze the power imbalance in the digital environment as a fundamental factor of causing harm online.

Methods: the work uses a conceptual and analytical methodology based on an interdisciplinary analysis of the theoretical provisions of law, technoethics, philosophy of technology, and social psychology. The methodological tools are complemented by constructing unique conceptual models through analyzing the structural factors of the digital space, developing causal relationships and creating a taxonomy of cyberbullying forms. Special attention is paid to the comparative analysis of regulatory approaches of different jurisdictions and the identification of gaps in existing legal norms.

Results: the research established that cyberbullying is a complex multilevel phenomenon that occurs at the intersection of the architectural features of digital platforms, the asymmetry of technological competencies between participants in interactions, and the systemic fragmentation of legislative regulation. It identified the critical gaps in key international legal instruments, manifested in the lack of unified definitions of cyberbullying, insufficiently elaborated mechanisms for cross-border cooperation, and irrelevant addressing of the digital environment specifics. The author analyzed the fundamental ethical issues related to automated content moderation based on machine learning algorithms, the distribution of responsibility between platforms, government regulators and individual users, and the contradictions between ensuring security and maintaining user autonomy. Four main types of power imbalances were identified: technological, informational, social, and institutional; each of them requires specific strategies to overcome.

Scientific novelty: for the first time, the article proposed a comprehensive approach to analyzing cyberbullying as a structurally determined abuse of digital power through the prism of technoethics. The developed conceptual models provide new tools for understanding the distributed nature of responsibility in the digital ecosystem and forming ethically sound prevention strategies. The author introduced a concept of information misuse as a central mechanism of systematic abuse of power in the digital environment.

Practical significance: the research is aimed at legal scholars, public officials, and digital platform developers. It offers practical solutions in the fields such as ethical audit of algorithms, creation of hybrid moderation systems involving artificial intelligence and humans, formation of international task forces, and development of human rights-based principles of digital literacy. The author's proposals may help to create a safer, more accountable and inclusive digital environment for all participants.

For citation

Spyropoulos, F. (2025). Techno-Ethical and Legal Aspects of Cyberbullying: Structural Analysis of Power Imbalances in the Digital Sphere. *Journal of Digital Technologies and Law, 3*(3), 472–496. https://doi.org/10.21202/jdtl.2025.19

References

Bosworth, K., Espelage, D. L., & Simon, T. R. (1999). Factors associated with bullying behavior in middle school students. *The Journal of Early Adolescence*, *19*(3), 341–362. https://doi.org/10.1177/0272431699019003003

Chakraborty, S., Bhattacherjee, A., & Onuchowska, A. (2021). Cyberbullying: A review of the literature. SSRN. http://dx.doi.org/10.2139/ssrn.3799920

Campbell, M., & Bauman, S. (2018). Cyberbullying: Definition, consequences, prevalence. In M. Campbell & S. Bauman (Eds.), *Reducing Cyberbullying in Schools* (pp. 3–16). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00001-8

Capurro, R. (2009). Digital ethics. *The Information Society*, *25*(3), 183–186. https://doi.org/10.1080/01972240902848902

Chen, C. W. Y. (2017). "Think before you type": The effectiveness of implementing an anti-cyberbullying project in an EFL classroom. *Pedagogies*, *13*(1), 1–18. https://doi.org/10.1080/1554480X.2017.1363046

Courakis, N. (2005). *Criminological horizons. Vol. II: Pragmatic approach and individual issues*. 2nd ed. Athens – Komotini: Ant. N. Sakkoula (In Greek).

Duncan, S. H. (2016). Cyberbullying and restorative justice. In R. Navarro, S. Yubero & E. Larrañaga (Eds.). *Cyberbullying Across the Globe* (pp. 239–257). Cham: Springer International Publishing.

Englander, E., Donnerstein, E., Kowalski, R., Lin, C. A., & Parti, K. (2017). Defining cyberbullying. *Pediatrics*, *140*(Supplement_2), S148–S151. https://doi.org/10.1542/peds.2016-1758u

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford: Oxford University Press.

Furnell, S. M. (2006). *Computer Insecurity: Risking the System*. Oxford: Chandos Publishing.

Gibson, J. J. (2014). The theory of affordances (originally published 1979). In G. Bridge & S. Watson (Eds.). *The People, Place, and Space Reader* (pp. 56–60). London: Routledge.

Guardabassi, V., & Nicolini, P. (2024). Adolescence and cyberbullying: a restorative approach. In *INTED2024 Proceedings* (pp. 4562–4570). IATED. https://doi.org/10.21125/inted.2024.1183

Hasan, M. T., Hossain, M. A. E., Mukta, M. S. H., Akter, A., Ahmed, M., & Islam, S. (2023). A review on deep-learning-based cyberbullying detection. *Future Internet*, *15*(5), 179. https://doi.org/10.3390/fi15050179

Hinduja, S., & Patchin, J. W. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice*, *4*(2), 148–169. https://doi.org/10.1177/1541204006286288

Hinduja, S., & Patchin, J. W. (2009). *Bullying beyond the schoolyard: Preventing and responding to cyberbullying*. Thousand Oaks, CA: Sage Publications.

Ioannou, A., Blackburn, J., Stringhini, G., De Cristofaro, E., Kourtellis, N., & Sirivianos, M. (2018). From risk factors to detection and intervention: a practical proposal for future work on cyberbullying. *Behaviour & Information Technology*, *37*, 258–266. https://doi.org/10.1080/0144929X.2018.1432688

Johora, F. T., Khan, M. S. I., Kanon, E., Rony, M. A. T., Zubair, M., & Sarker, I. H. (2024). A data-driven predictive analysis on cyber security threats with key risk factors. *arXiv preprint arXiv:2404.00068*.

Juvonen, J., & Gross, E. F. (2008). Extending the school grounds? Bullying experiences in cyberspace. *Journal of School Health*, *78*(9), 496–505. https://doi.org/10.1111/j.1746-1561.2008.00335.x

Katerelos, I., Tsekeris, C., Lavdas, M., & Demetriou, K. (2011). A psychosociological approach to Internet use and mass online role-playing games. In K. Siomos & G. Floros (Eds.), *Research, prevention, management of risks in Internet use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Kim, S., Razi, A., Stringhini, G., Wisniewski, P. J. and De Choudhury, M. (2021). A human-centered systematic literature review of cyberbullying detection algorithms. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2). https://doi.org/10.1145/3476066

Kowalski, R. (2018). Cyberbullying. In J. P. Forgas, R. F. Baumeister & T. F. Denson (Eds.), *The Routledge International Handbook of Human Aggression* (pp. 131–142). London: Routledge. https://doi.org/10.4324/9781315618777-11

Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, *15*(6), 285–289. https://doi.org/10.1089/cyber.2011.0588

Lazos, G. (2001). *Information Technology and Crime*. Athens: Nomiki Bibliothiki. (In Greek).

Li, Q. (2007). New bottle but old wine: A research of cyberbullying in schools. *Computers in Human Behavior*, *23*(4), 1777–1791. https://doi.org/10.1016/j.chb.2005.10.005

Luppicini, R. (2018). *The Changing Scope of Technoethics in Contemporary Society*. Hershey, PA: Information Science Reference. https://doi.org/10.4018/978-1-5225-5094-5

Meier, A., Reinecke, L., & Meltzer, C. E. (2016). "Facebocrastination"? Predictors of using Facebook* for procrastination and its effects on students' well-being. *Computers in Human Behavior*, *64*, 65–76. https://doi.org/10.1016/j.chb.2016.06.011

Menesini, E., Nocentini, A., & Palladino, B. E. (2012). Empowering students against bullying and cyberbullying: Evaluation of an Italian peer-led model. *International Journal of Conflict and Violence*, *6*(2), 313–320. https://doi.org/10.4119/ijcv-2922

Menesini, E., Nocentini, A., & Camodeca, M. (2013). Morality, values, traditional bullying, and cyberbullying in adolescence. *British Journal of Developmental Psychology*, *31*(1), 1–14. https://doi.org/10.1111/j.2044-835X.2011.02066.x

Millard, G. (2009). Stephen Harper and the politics of the bully. *Dalhousie Review*, *89*(3), 329–336.

Moor, J. H. (2005). Why we need better ethics for emerging technologies. *Ethics and Information Technology*, *7*(3), 111–119. https://doi.org/10.1007/s10676-006-0008-0

Mouzaki, D. (2010). International scientific conference on: "Dealing with cyberbullying from a legal perspective". *The Art of Crime*, *15*. (In Greek).

Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. *Australian Journal of Guidance & Counselling*, *20*(2), 129–142. https://doi.org/10.1375/ajgc.20.2.129

Olweus, D. (1993). *Bullying at School: What We Know and What We Can Do*. Oxford, UK: Blackwell.

Ortega-Ruiz, R., Del Rey, R., & Casas, J. A. (2012). Knowing, building and living together on internet and social networks: the ConRed cyberbullying prevention program. *International Journal of Conflict and Violence*, *6*(2), 303–313. https://doi.org/10.4119/ijcv-2921

Othman, S. N., Alziboon, M. F., Dawood, M., Sachet, S. J., & Moroz, I. (2024). New rehabilitation against electronic crimes by young people. *Encuentros: Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico*, *22*, 363–385. https://doi.org/10.5281/zenodo.13732745

Raj, M., Singh, S., Solanki, K., & Selvanambi, R. (2022). An application to detect cyberbullying using machine learning and deep learning techniques. *SN Computer Science*, *3*(5), 401. https://doi.org/10.1007/s42979-022-01266-w

* The social network belongs to Meta, which is recognized as an extremist organization, its functioning is prohibited in the territory of the Russian Federation.

Sathya, J., & Fernandez, F. M. H. (2024). Predictive analysis in healthcare systems. In A. J. Anand, K. Kalaiselvi & J. M. Chatterjee (Eds.), *Artificial Intelligence – Based System Models in Healthcare* (pp. 131–152). Wiley. https://doi.org/10.1002/9781394242528.ch6

Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*, *49*(2), 147–154. https://doi.org/10.1111/j.1467-9450.2007.00611.x

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry*, *49*(4), 376–385. https://doi.org/10.1111/j.1469-7610.2007.01846.x

Smith, P. K., del Barrio, C., & Tokunaga, R. S. (2013). Definitions of bullying and cyberbullying: How useful are the terms? In S. Bauman, D. Cross & J. Walker (Eds.), *Principles of cyberbullying research: Definitions, measures, and methodology* (pp. 26–40). New York: Routledge/Taylor & Francis Group.

Spyropoulos, F. (2011). The manifestations of deviant behavior on the Internet – Reflections on the needs of modernization of Greek criminal legislation. In K. Siomos & G. Floros (Eds.), *Research, Prevention, Management of Risks in Internet Use*. Larissa: Hellenic Society for the Study of Internet Addiction Disorder. (In Greek).

Tavani, H. T. (2011). *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing* (3rd ed). Hoboken, NJ: Wiley.

Topcu-Uzer, C., & Tanrıkulu, İ. (2018). Technological solutions for cyberbullying. In M. Campbell & S. Bauman (Eds.), *Reducing cyberbullying in schools* (pp. 33–47). Academic Press. https://doi.org/10.1016/B978-0-12-811423-0.00003-1

Tsouramanis, Ch. (2005). *Digital Crime – The (Un)Safe Side of the Internet*. Athens: V. Katsaros Publications. (In Greek).

Vandebosch, H. (2019). Cyberbullying prevention, detection and intervention. In W. Heirman, M. Walrave & H. Vandebosch (Eds.), *Narratives in Research and Interventions on Cyberbullying among Young People* (pp. 29–44). Cham: Springer. https://doi.org/10.1007/978-3-030-04960-7_3

Vandebosch, H., & Van Cleemput, K. (2008). Defining cyberbullying: A qualitative research into the perceptions of youngsters. *CyberPsychology & Behavior*, *11*(4), 499–503. https://doi.org/10.1089/cpb.2007.0042

Verbeek, P.-P. (2011). *Moralizing Technology: Understanding and Designing the Morality of Things*. Chicago: University of Chicago Press. https://doi.org/10.7208/chicago/9780226852904.001.0001

Ybarra, M. L., & Mitchell, K. J. (2004a). Online aggressors/targets, aggressors, and targets: A comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry*, *45*, 1308–1316. https://doi.org/10.1111/j.1469-7610.2004.00328.x

Ybarra, M. L., & Mitchell, K. J. (2004b). Youth engaging in online harassment: Associations with caregiver-child relationships, Internet use, and personal characteristics. *Journal of Adolescence*, *27*, 319–336. https://doi.org/10.1016/j.adolescence.2004.03.007

Zannis, A. (2005). *Cybercrime*. Athens-Komotini: Sakkoulas Publications. (In Greek).

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Author information

Fotios Spyropoulos – PostDoc, PhD, Associate Professor of Criminal Law & Criminology, Faculty of Law, Philips University; Senior Partner of Spyropoulos Law Firm
Address: 4-6 Lamias Street, 2001, P.O. Box 28008, Nicosia, Cyprus; Alexandras Avenue 81, 11474, Athens, Greece
E-mail: fspyropoulos@gmail.com
ORCID ID: https://orcid.org/0000-0001-5950-3583
Google Scholar ID: https://scholar.google.com/citations?user=iKQYLWoAAAAJ

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 29, 2025
Date of approval – June 12, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика

Гергана Варбанова

Высшее военно-морское училище имени Николы Вапцарова, Варна, Болгария

Ключевые слова

аутентичность,
вещественные доказательства,
доказательства,
европейское законодательство,
право,
процессуальные действия,
судебное разбирательство,
цифровая информация,
цифровые технологии,
электронные доказательства

Аннотация

Цель: исследование направлено на разработку новой теоретической основы, которая бросает вызов традиционной классификации электронных доказательств как подвида вещественных доказательств и предлагает рассматривать их как качественно новый правовой феномен с собственной независимой правовой природой в контексте применимого европейского законодательства.

Методы: в работе применяется доктринальный метод для юридического анализа применимых европейских нормативных актов, включая Регламент (ЕС) 2023/1543 и Регламент (ЕС) 910/2014 (eIDAS), и их непосредственного применения в национальных правовых системах государств – членов Европейского союза. Для выявления различий между теоретическими взглядами и прецедентным правом используется сравнительно-правовой подход. Проводится технологический анализ цифровой информации и поясняются конкретные примеры, иллюстрирующие проблемы, связанные со сбором и использованием электронных доказательств в рамках европейского законодательства.

Результаты: автор предлагает новое доктринальное понимание электронных доказательств как самостоятельной категории доказательств, отличающейся от традиционных вещественных доказательств цифровой природой и специфическими характеристиками. Внедрение европейских регламентов требует переосмысления правовой природы электронных доказательств как качественно отличного правового явления. Установлено, что отношение к электронным доказательствам как к вещественным создает риск правовой неопределенности, а отсутствие соответствующего правового регулирования препятствует эффективному правоприменению.

Научная новизна: в исследовании впервые предлагается преодолеть устоявшуюся парадигму и выделить электронные доказательства как самостоятельную правовую категорию в системе видов доказательств. Обосновывается уникальная цифровая природа электронных

доказательств и необходимость создания независимой правовой базы в различных национальных законодательствах. Предложено совершенствование научной терминологии с использованием термина «электронные доказательства», соответствующего юридическим определениям в рассматриваемых нормативных правовых актах, вместо устаревшего термина «цифровые доказательства».

Практическая значимость: работа содержит конкретные рекомендации практического характера для использования электронных доказательств в процедурах их идентификации, хранения, представления и анализа в различных судебных разбирательствах в соответствии с применимым наднациональным законодательством. Исследование способствует преодолению устаревших представлений о правовой природе электронных доказательств и их неверного отождествления с вещественными доказательствами, что имеет важное значение для эффективного правоприменения в государствах – членах Европейского союза.

Для цитирования

Варбанова, Г. (2025). Электронные доказательства как самостоятельный правовой феномен: теоретические основы и европейская практика. *Journal of Digital Technologies and Law*, *3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

Содержание

Введение

Электронные доказательства имеют особую природу, что отличает их от других видов доказательств, существующих в аналоговом мире. Это подтверждается фактами, которые имели место в прошлом, но относятся и к настоящему. Особенность электронных доказательств заключается в том, что они сохраняются неизменными в течение длительного периода времени, однако для них характерна и динамика, т. е. их содержание может отличаться от состояния в момент существования факта, который они удостоверяют. Часто содержание электронных доказательств изменяют, чтобы скрыть информацию или намеренно исказить ее, и отследить эти изменения нелегко. Электронные доказательства содержат цифровую информацию, закодированную в виде двоичных данных (последовательности единиц и нулей), и это бросает вызов юридической теории и практике, поскольку юридическая наука оказывается неразрывно связанной с техническими особенностями электронных доказательств

как нового правового феномена. Цифровую информацию нельзя рассматривать как материальный объект, ее нельзя воспринимать непосредственно, она не является объектом физического мира. Все это создает серьезные проблемы для юридической теории и практики.

В статье представлена новая теоретическая база, позволяющая пересмотреть традиционную классификацию электронных доказательств как подмножества вещественных доказательств. Автор предлагает изменить парадигму понимания правовой природы электронных доказательств и рассматривает их как новое правовое явление, имеющее свою собственную независимую правовую природу и требующее наднационального регулирования. Исследование фокусируется на применимом европейском законодательстве, включая Регламент (ЕС) 2023/1543, Регламент (ЕС) 910/2014 (eIDAS), и на тех проблемах, которые ставит перед нами указанная новая теория правовой природы электронных доказательств.

В работе использован доктринальный метод правового анализа применимых нормативных актов ЕС и практики их применения в национальных правовых системах государств Евросоюза. Для прояснения различий между теоретическими положениями и прецедентным правом, возникающих при применении наднациональных правовых норм, применяется сравнительный подход. Автор анализирует технологические аспекты, связанные с природой цифровой информации, и приводит конкретные примеры, иллюстрирующие проблемы, связанные со сбором и использованием электронных доказательств в контексте европейского законодательства.

В статье предпринята попытка предложить пути преодоления старой парадигмы и выделить электронные доказательства в качестве самостоятельной правовой категории в системе видов доказательств, а также отграничить их от вещественных доказательств. Приводятся аргументы в пользу уникальной цифровой природы электронных доказательств и необходимости создания независимой правовой базы в рамках национальных законодательств. Автор предлагает усовершенствовать научную терминологию, а именно использовать термин «электронные доказательства», который соответствует юридическим определениям, приведенным в рассматриваемых нормативных актах, и отказаться от использования устаревшего термина «цифровые доказательства».

1. Классическая теория вещественных доказательств

Данная теория определяет вещественные доказательства как материальные объекты, которые воспроизводят факты, имеющие отношение к делу, или позволяют делать доказательные выводы об этих фактах. Они относятся к событиям, которые произошли в прошлом, но имеют значение в настоящем и связаны с процессом доказывания. Например, Mubarik (2019) рассматривает в качестве вещественных доказательств любые предметы, материалы, отпечатки пальцев и различные вещества (в том числе телесные), собранные на месте преступления, которые имеют отношение к расследованию и могут способствовать прояснению обстоятельств дела. Чтобы доказательство можно было квалифицировать как вещественное, оно должно иметь материальную природу и восприниматься с помощью органов чувств человека. Некоторые теоретики утверждают, что физический носитель несет цифровую информацию (например, диск, USB-носитель, жесткий диск), а значит, может рассматриваться как вещественное доказательство (Pastukhov, 2015; Dmitrieva & Pastukhov, 2023).

Этот традиционный подход имеет недостатки и подвергается серьезной критике, поскольку электронные доказательства, рассматриваемые в качестве цифровой информации, не всегда имеют материальную природу и могут существовать исключительно в цифровой среде, не будучи объективированными на физическом носителе – например, в виде записи на облачном сервере. Электронные доказательства часто не существуют в аналоговой форме и не являются частью материального мира в классическом смысле этого слова.

2. Европейское законодательство, применимое к электронным доказательствам

Стремясь определить и унифицировать понимание специфической правовой природы электронных доказательств, Европейский союз принял Регламент (ЕС) 2023/1543, который имеет прямое применение и содержит юридическое определение понятия «электронные доказательства». Такое законодательное решение не случайно, оно направлено на преодоление различий в толковании понятий в национальных законодательствах государств-членов и на достижение единого понимания правовой природы электронных доказательств.

Регламент определяет «электронные доказательства» как данные абонента, данные о трафике или данные о контенте, хранящиеся поставщиком услуг или от имени поставщика услуг в электронной форме. Этот законодательный подход отличается нейтральностью и не содержит исчерпывающего перечня всех видов цифровой информации, которые могут быть квалифицированы как электронные доказательства. Регламент выделяет лишь электронные доказательства как особый вид цифровой информации, которая хранится или передается поставщиками услуг в контексте предоставления ими цифровых услуг и для целей уголовного судопроизводства. Файлы или другие цифровые данные, хранящиеся пользователями локально, не подпадают под действие Регламента (ЕС) 2023/1543. Такие данные могут подпадать под определение «электронных документов» в соответствии с Регламентом (ЕС) 910/2014 (eIDAS), если они содержат информацию, имеющую юридическое значение для различных гражданских, коммерческих, административных или иных общественных отношений.

Регламент (ЕС) 910/2014 (eIDAS) определяет «электронный документ» как любой контент, хранящийся в электронной форме, в частности, в виде текста, звукозаписи, изображения или аудиовидеозаписи. В контексте eIDAS электронный документ – это носитель цифровой информации, относящейся к гражданским, административным, коммерческим или иным общественным отношениям. Достаточным условием является содержание в электронном документе информации, имеющей юридическое значение, независимо от того, был ли документ создан случайно или намеренно для целей конкретного правоотношения. Статья 46 Регламента (ЕС) 910/2014 предусматривает, что электронный документ имеет такую же доказательственную ценность, как и другие виды доказательств. Цитируемая норма императивно гласит, что недопустимо отрицать доказательственную ценность электронного документа только потому, что он представлен в электронной форме. Это, в свою очередь, обеспечивает правовую определенность в трансграничных спорах, включая арбитраж (Ferreira & Gromova, 2024). На практике Регламент обязывает государства-члены признавать действительность электронных документов в качестве

допустимых доказательств в различных судебных разбирательствах (Nekrošius, 2021; Daniel & Daniel, 2012)[1].

В контексте нашего исследования следует сравнить понятия «электронное доказательство» по смыслу Регламента (ЕС) 2023/1543 и «электронный документ» по смыслу Регламента (ЕС) 910/2014. Электронные доказательства в соответствии с Регламентом (ЕС) 2023/1543 охватывают широкий спектр цифровой информации – данные об абонентах, трафике и контенте, которые могут включать структурированные или неструктурированные данные, метаданные или содержание сообщений – и отличаются от электронных документов. Сфера действия Регламента (ЕС) 2023/1543 ограничена конкретными делами в уголовном судопроизводстве – хранением и предоставлением электронных доказательств, и только в отношении цифровой информации, хранящейся поставщиками услуг или от их имени.

С другой стороны, понятие «электронный документ» по смыслу Регламента (ЕС) 910/2014 (eIDAS) имеет более узкое технологическое применение, поскольку оно, по сути, относится к цифровому контенту, воспринимаемому как «документ», но его юридическая применимость значительно шире. «Электронный документ» не ограничивается сферой уголовного судопроизводства или данными, хранящимися у конкретных поставщиков услуг, но применим ко всем отраслям права: гражданскому, коммерческому, административному и уголовному (Kirkov, 2022; Berube et al., 2025; Shin et al., 2025). Поэтому можно сделать вывод, что электронные доказательства в соответствии с Регламентом 2023/1543 представляют собой специализированный тип цифровой информации, предназначенной для целей уголовного судопроизводства, и имеют более узкую сферу регулирования. Напротив, электронные документы в соответствии с Регламентом 910/2014 имеют более широкую сферу применения и значение, поскольку их допустимость в качестве доказательств зависит не от конкретного контекста уголовного судопроизводства, не от места хранения или источника данных, а от соблюдения принципов, установленных законодательством ЕС для процессов электронной идентификации, аутентификации и доверительных услуг, включая типы электронных подписей, используемых в электронных документах.

Примечательно сходство определений «данных контента» в Регламенте (ЕС) 2023/1543 и «электронных документов» в eIDAS. Разница заключается в контексте и целях: «данные контента» в соответствии с Регламентом 2023/1543 ориентированы на цифровую информацию, которая передается и хранится поставщиками цифровых услуг и которая должна храниться и, соответственно, предоставляться для нужд уголовного правосудия, в то время как определение «электронного документа» в eIDAS относится к признанию юридической ценности и использованию электронных документов во всех сферах общественной жизни.

Определение электронных доказательств по смыслу Регламента (ЕС) 2023/1543 не является исчерпывающим, а лишь описывает некоторые виды цифровой информации, которые могут рассматриваться как электронные доказательства. Этот подход идентичен определению понятия «электронный документ» в Регламенте (ЕС) 910/2014 – любой контент, хранящийся в электронной форме, в частности текст, звукозапись, изображение или аудиовизуальная запись. В обоих случаях перечень не является исчерпывающим, ведь технологии развиваются. При регулировании

[1] Varbanova, G. (2020). Legal regime of electronic documents. Varna: Dangrafik Publishing.

общественных отношений в сфере информационных технологий законодательный подход должен быть гибким, учитывая динамику технологического развития. Технологическое развитие подразумевает появление новых типов электронных доказательств и электронных документов, которые нельзя исключить из сферы действия Регламента (ЕС) 2023/1543 или eIDAS просто потому, что они не определены в явном виде как электронные доказательства или электронные документы соответственно.

3. Определение и правовая природа электронных доказательств

Электронные доказательства – это один из ключевых инструментов в процессе доказывания, который требует особого подхода к их сбору, анализу и правовой оценке. Такой подход должен учитывать интенсивное развитие технологий, а также специфические особенности электронных доказательств в контексте процесса нормотворчества (Begishev et al., 2020).

До принятия Регламента (ЕС) 2023/1543 теоретические исследования определяли электронные доказательства как любую информацию, хранящуюся или передаваемую в цифровой форме, которая может быть использована в качестве доказательства. Традиционно некоторые авторы считают электронные доказательства вещественными, поскольку содержащаяся в них информация объективирована на конкретном материальном носителе. Согласно этому подходу, доказательственную ценность определяют физические характеристики носителя, а не сама информация (электронные доказательства), записанная на нем. Несмотря на кажущуюся правдоподобность, эта концепция является ошибочной, поскольку не учитывает и не отражает специфическую природу электронных доказательств как цифровой информации, которая обладает своими уникальными характеристиками (Wu et al., 2025)[2].

В более поздних исследованиях также высказывается представление о том, что электронные документы являются особой категорией квазивещественных доказательств. По мнению ряда авторов (Bufetova, 2023; Guo, 2022), электронный документ в качестве вещественного доказательства – это документ, который существует в электронном виде, содержит информацию, относящуюся к делу, и записан на электронном носителе, позволяющем воспроизводить и использовать эту информацию в процессе доказывания. Это определение показывает, что электронный документ принадлежит к особому виду квазивещественных доказательств, в котором важна информация, содержащаяся на материальном носителе, а не его материальные характеристики.

Такая неопределенность возникает из-за непонимания того, как создается, изменяется, хранится и удаляется цифровая информация. Цифровая информация может храниться на различных носителях: жестком диске, USB-устройстве, в облаке, на сервере – или передаваться по электронным каналам, но информация не идентична самому носителю. Файл может быть сохранен на компьютере или другом техническом носителе, скопирован, передан или удален, но компьютер или носитель, на котором записан файл, не является вещественным доказательством, тем более что

[2] Varbanova, G. (2024). The significance of electronic evidence in the context of cybersecurity and national security. Print Master Publishing.

информация может быть записана на облачном сервере и доступна через компьютер или другое устройство.

Из определений электронных доказательств и электронных документов видно, что они не имеют материальной (осязаемой) природы, а представляют собой цифровую запись, поэтому их можно определить как разновидность нематериальных доказательств (Vuchkov, 2023; Horsman, 2021). Для того чтобы иметь возможность определить электронные доказательства как новое правовое явление, необходимо прояснить их цифровую природу и способ создания, передачи, хранения, записи и удаления цифровой информации.

Цифровая информация – это данные в двоичном коде, последовательность нулей и единиц, обрабатываемая информационными системами (компьютером, интеллектуальным устройством и т. д.). Таким образом, текст, изображения, звук или видео, записанные на техническом носителе, представляют собой цифровую информацию в двоичном коде, которая может быть воспринята органами чувств человека с помощью обычных средств через использование общепринятых стандартов преобразования и воспроизведения информации, с помощью которых нули и единицы могут восприниматься в виде текста, изображений или аудиофайлов.

Чтобы собранные электронные доказательства был приняты в суде, необходимо обеспечить полную целостность и идентичность информационных данных, с тем чтобы гарантировать их подлинность, целостность содержания и неизменность данных. Только при соблюдении этих требований электронные доказательства могут быть приняты в качестве действительных и надежных доказательств в судебном разбирательстве.

4. Аутентичность, целостность и доказательное значение электронных документов

Для современного мира характерно постоянное увеличение числа правоотношений, которые возникают, развиваются и прекращаются в электронной среде. Каждый день исключительно в электронном виде заключается множество контрактов, потребители пользуются онлайн-сервисами, совершают электронные платежи, и даже судебные разбирательства теперь проводятся с помощью видеоконференций и других инструментов электронного мира. Практически все сферы общественной и экономической жизни тесно связаны с использованием электронных средств коммуникации, обработки и хранения информации.

Киберпространство стало зоной коммерции, которая выходит за рамки физических границ, но в то же время представляет собой центр притяжения для совершения многочисленных новых и ранее неизвестных компьютерных преступлений.

Электронные доказательства – будь то электронные документы, записи актов коммуникации, лог-файлы, метаданные или другие формы цифровой информации – являются неотъемлемой частью правовых отношений в электронной среде и имеют существенное значение для раскрытия преступлений, совершаемых в киберпространстве. Для доказывания фактов, независимо от того, идет ли речь о гражданских или коммерческих правоотношениях или о преступлениях, совершенных в киберпространстве, требуется гарантировать подлинность, целостность и неизменность электронных доказательств. Это достигается путем применения соответствующих технических и организационных мер.

Ключевой проблемой при представлении, анализе и принятии электронных доказательств в ходе судебных разбирательств (гражданских, уголовных или административных) являются подлинность, целостность и доказательная ценность электронных доказательств и электронных документов. В современном цифровом мире электронные доказательства становятся наиболее часто используемыми доказательствами. Для того чтобы быть принятыми в качестве действительных и надежных средств доказывания, электронные доказательства и электронные документы должны удовлетворять нескольким критериям, включая обеспечение целостности цифровых данных, чтобы гарантировать их подлинность, целостность и неизменность.

Электронный документ считается аутентичным, когда установлены автор, место и время его создания, а его содержание действительно исходит от указанного автора и не изменялось с момента его создания (Surovtseva, 2020). В этом смысле подлинность и неизменность электронного документа могут быть обеспечены за счет использования сертификационных услуг в соответствии с Регламентом (ЕС) 910/2014 (eIDAS) – например, квалифицированной электронной подписи, квалифицированной электронной печати или квалифицированного электронного штампа времени, которые удостоверяют как личность автора, так и время создания и целостность электронного документа. Целостность электронного документа или цифровой информации также может быть гарантирована за счет использования технологии блокчейн- и смарт-контрактов, которые обеспечивают возможность хранения данных в децентрализованной, неизменяемой и прозрачной среде (Miao et al., 2021). Записи в реестре блокчейна гарантируют, что содержание электронного документа не подвергалось изменениям с момента его создания. Данная технология обеспечивает надежное хранение электронного документа, защиту от его последующего изменения или удаления, а также удостоверяет хронологию записей в децентрализованном реестре, что гарантирует подлинность и отслеживаемость электронных доказательств (Al-E'mari et al., 2024; Stoykova, 2023).

Системы искусственного интеллекта также могут использоваться в процессе доказывания, и в частности на этапе проверки подлинности электронных документов, посредством автоматизированного анализа содержимого, обнаружения аномалий, сравнения версий и оценки рисков, что повышает безопасность работы с электронными доказательствами. Интеграция систем искусственного интеллекта, блокчейн-технологий и служб квалифицированной сертификации создает многоуровневый механизм защиты целостности и подлинности электронных документов и электронных доказательств, особенно в контексте судебных разбирательств и электронного правосудия.

Заключение

В данном исследовании предлагается изменить традиционную парадигму понимания правовой природы электронных доказательств в контексте европейского законодательства. Проанализированы Регламент (ЕС) 2023/1543 и Регламент (ЕС) 910/2014 (eIDAS); метод сравнительно-правового анализа позволяет сделать вывод о том, что электронные доказательства нельзя приравнивать к традиционной категории вещественных доказательств, поскольку они имеют особую, цифровую природу и уникальные технические характеристики. Электронные доказательства – это новый правовой феномен, который должен получить самостоятельное правовое регулирование

в отношении процессуальных действий, связанных с их сбором, хранением, анализом и принятием в качестве адекватного средства доказывания в судебном процессе. Рассмотрение электронных доказательств в качестве одного из видов вещественных доказательств не только неверно, но и создает реальный риск правовой неопределенности и трудностей в эффективном правоприменении в отдельных государствах – членах ЕС. Настоящее исследование способствует развитию теоретического понимания электронных доказательств в соответствии с применимым европейским законодательством, а также намечает возможности для будущих исследований по интеграции новых технологий, таких как блокчейн и искусственный интеллект, в процесс доказывания и верификации подлинности электронных доказательств.

В работе предлагается преодолеть старую парадигму и выделить электронные доказательства как самостоятельную правовую категорию в системе видов доказательств, а также установить их отличия от вещественных доказательств. Автор приводит ряд аргументов в пользу уникальной цифровой природы электронных доказательств и необходимости создания независимой правовой базы в различных национальных законодательствах. Предлагается усовершенствовать научную терминологию, используя термин «электронные доказательства», который соответствует юридическим определениям, приведенным в рассматриваемых нормативных актах, и отказаться от использования устаревшего термина «цифровые доказательства».

Автор приводит конкретные рекомендации, имеющие практическое значение в процессе использования электронных доказательств, а именно идентификации, хранения, представления и анализа электронных доказательств в различных судебных разбирательствах в соответствии с применимым наднациональным законодательством. В то же время в данном исследовании предлагается преодолеть устаревшие представления о правовой природе электронных доказательств и их неверное отождествление с вещественными доказательствами.

Список литературы

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Информация об авторе

Варбанова Гергана – PhD, ассистент кафедры права в области национальной безопасности и информационных технологий, Высшее военно-морское училище имени Николы Вапцарова
Адрес: Болгария, г. Варна, ул. Василя Друмева, д. 73
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

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: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 19 июня 2025 г.
Дата одобрения после рецензирования – 28 июня 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:347:004.4
EDN: https://elibrary.ru/jqhnur
DOI: https://doi.org/10.21202/jdtl.2025.20

Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice

Gergana Varbanova
Nikola Vaptsarov Naval Academy, Varna, Bulgaria

Keywords

authenticity,
digital information,
digital technologies,
electronic evidence,
European legislation,
evidence,
judicial procedure,
law,
material evidence,
procedure

Abstract

Objective: to develop a new theoretical framework that challenges the traditional classification of electronic evidence as a subtype of material evidence and suggests considering it as a qualitatively new legal phenomenon with its own independent legal nature in the context of applicable European legislation.

Methods: the work uses the doctrinal method for the legal analysis of applicable European legislation, including Regulation (EU) 2023/1543 and Regulation (EU) 910/2014 (eIDAS), as well as their direct application in the national legal systems of the European Union member states. A comparative legal approach was used to identify differences between theoretical views and case law. A technological analysis of digital information was performed; specific examples were explained to illustrate the problems associated with the collection and use of electronic evidence within the European legislation framework.

Results: the author proposes a new doctrinal understanding of electronic evidence as an independent category that differs from traditional material evidence in its digital nature and specific characteristics. The introduction of European regulations requires rethinking the legal nature of electronic evidence as a qualitatively different legal phenomenon. It was established that treating electronic evidence as material one creates a risk of legal uncertainty, while the lack of appropriate legal regulation hinders effective law enforcement.

Scientific novelty: for the first time, the research proposes to overcome the established paradigm and identify electronic evidence as an independent

legal category in the system of evidence types. The article substantiates the unique digital nature of electronic evidence and the need to create an independent legal framework in various national legislations. It is proposed to improve scientific terminology using the term "electronic evidence", which corresponds to the legal definitions in the legislation under study, instead of the outdated term "digital evidence".

Practical significance: the work contains specific practical recommendations for the use of electronic evidence in the procedures for its identification, storage, presentation and analysis in various court proceedings in accordance with applicable supranational legislation. The research helps to overcome outdated ideas about the legal nature of electronic evidence and their incorrect identification with material evidence. This is important for effective law enforcement in the European Union member states.

For citation

Varbanova, G. (2025). Electronic Evidence as an Independent Legal Phenomenon: Theoretical Framework and European Practice. *Journal of Digital Technologies and Law, 3*(3), 497–511. https://doi.org/10.21202/jdtl.2025.20

References

Al-E'mari, S., Sanjalawe, Y., Makhadmeh, S., & Alqudah, H. (2024). Digital forensics meets blockchain: Enhancing evidence authenticity and traceability. *2024 2nd International conference on cyber resilience (ICCR)* (pp. 01–06). IEEE. https://doi.org/10.1109/ICCR61006.2024.10532961

Begishev, I. R., Khisamova, Z. I., & Nikitin, S. G. (2020). The organization of hacking community: Criminological and criminal law aspects. *Russian Journal of Criminology*, *14*(1), 96–105. (In Russ.). https://doi.org/10.17150/2500-4255.2020.14(1).96-105

Bérubé, M., Beaulieu, L., Allard, S., & Denault, V. (2025). From digital trace to evidence: Challenges and insights from a trial case study. *Science & Justice*, *65*(5), 101306. https://doi.org/10.1016/j.scijus.2025.101306

Bufetova, M. Sh. (2023). The electronic document as a type of physical evidence in Russian criminal proceedings. *Siberian Legal Readings*, *3*, 47–55. https://doi.org/10.17150/2411-6122.2023.3.47-55

Daniel, Larry. E., & Daniel, Lars. E. (2012). *Discovery of digital evidence in civil cases. In Digital Forensics for Legal Professionals* (Ch. 16, pp. 113–121). Elsevier eBooks. https://doi.org/10.1016/b978-1-59749-643-8.00016-x

Dmitrieva, A. A., & Pastukhov, P. S. (2023). Concept of Electronic Evidence in Criminal Legal Procedure. *Journal of Digital Technologies and Law*, *1*(1), 270–295. https://doi.org/10.21202/jdtl.2023.11

Ferreira, D., & Gromova, E. (2024). Digital evidence in disputes involving states. *AJIL Unbound*, *118*, 51–56. https://doi.org/10.1017/aju.2024.4

Guo, Z. (2022). Regulating the use of electronic evidence in Chinese courts: Legislative efforts, academic debates and practical applications. *Computer Law & Security Review*, *48*, 105774. https://doi.org/10.1016/j.clsr.2022.105774

Horsman, G. (2021). Digital evidence and the crime scene. *Science & Justice*, *61*(6), 761–770. https://doi.org/10.1016/j.scijus.2021.10.003

Kirkov, A. (2022). Forensic activity experts in Bulgaria. Organization and problems. In *Collection of materials international scientific and practical seminar on the topic: "Digitalization of activities Courts: Current and Prospective Tasks"* (AI No. 276, 15.06.2015, pp. 5–9).

Miao, Z., Ye, C., Yang, P., Chen, Y., & Chen, Y. (2021). Blockchain-based Electronic Evidence Storage and Efficiency Optimization. In *2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT)* (pp. 109–113). IEEE. https://doi.org/10.1109/AIBT53261.2021.00025

Mubarik, N. (2019). Importance and role of physical evidence in forensic science. *Academic Journal of Forensic Sciences*, *2*(1), 18–22.

Nekrošius, V. (2021). Use of information technologies in Lithuanian civil procedure. *Procedia Computer Science*, *192*, 2662–2667. https://doi.org/10.1016/j.procs.2021.09.036

Pastukhov, P. S. (2015). Elektronnoe important evidence in a criminal case sudoproizvodstve. *Vestnik Tomsk state-owned University*, *396*, 149–153.

Shin, D., Ha, J., & Euom, I. (2025). Data-Driven Digital evidence analysis for the forensic investigation of the electric vehicle charging infrastructure. *Computer Modeling in Engineering & Sciences*, *143*(3), 3795–3838. https://doi.org/10.32604/cmes.2025.066727

Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review*, *49*, 105801. https://doi.org/10.1016/j.clsr.2023.105801

Surovtseva, N. (2020). Authenticity and identity of electronic records. *Herald of an archivist*, *2*, 467–477. https://doi.org/10.28995/2073-0101-2020-2-467-477

Vuchkov, V. (2023). Electronic evidence in criminal cases and its sources – necessary considerations. Law *Journal of New Bulgarian University*, *19*(2), 12–19. https://doi.org/10.33919/ljnbu.23.2.1

Wu, D., Zuo, X., & Guo, Y. (2025). The application of electronic evidence in forensic imaging analysis. *Journal of Radiation Research and Applied Sciences*, *18*(3), 101708. https://doi.org/10.1016/j.jrras.2025.101708

Author information

Gergana Varbanova – PhD, Assistant Professor, Department of National Security and Information Technology Law, Nikola Vaptsarov Naval Academy
Address: 73 Vasil Drumev Street, Varna, Bulgaria
E-mail: g.varbanova@naval-acad.bg
ORCID ID: https://orcid.org/0000-0001-8122-4353
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=60021317100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/HKP-1334-2023
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=02-0uFYAAAAJ

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 – June 99, 2025
Date of approval – June 28, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025

Научная статья
УДК 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия

Анумбуандем Бенволио Лекунзе

Университет Буэа, Буэа, Камерун

Ключевые слова

безопасность,
Камерун,
киберпреступность,
мошенничество,
право,
правосудие,
транзакции,
фишинг,
цифровые технологии,
электронная коммерция

Аннотация

Цель: проанализировать влияние киберпреступности на операции электронной коммерции в Камеруне и оценить эффективность существующих правовых механизмов противодействия киберугрозам.

Методы: исследование базируется на теориях утилитаризма, транзакционных издержек и рационального выбора. Применена методология качественного исследования с использованием доктринального метода. Проведен комплексный анализ правовых актов Камеруна в сфере кибербезопасности и электронной коммерции. Выполнено социологическое обследование с получением 250 выборочных ответов от жителей района Молико в городе Буэа в период с января по апрель 2025 г. Исследованы судебные прецеденты и статистические данные Министерства почты и телекоммуникаций Камеруна.

Результаты: установлено, что киберпреступления привели к потере доверия к операциям электронной коммерции в Камеруне, что отражается на снижении желания граждан осуществлять онлайн-транзакции. Выявлено, что более 60 % молодежи в возрасте от 16 до 35 лет в крупных городах Камеруна либо вовлечены в киберпреступления, связанные с электронной коммерцией, либо пострадали от них. Зафиксирован рост числа женщин среди киберпреступников. Определены основные виды киберпреступлений: мошенничество, фишинг и хищение средств с банковских карт.

Научная новизна: комплексный междисциплинарный анализ влияния киберпреступности на электронную коммерцию в контексте развивающейся африканской экономики. Впервые проведено эмпирическое исследование масштабов киберпреступности в конкретном регионе Камеруна с количественной оценкой вовлеченности молодежи в противоправную деятельность. Разработана теоретическая модель, объединяющая концепции утилитаризма, транзакционных издержек и рационального выбора для объяснения мотивации

киберпреступников. Выявлены специфические социально-правовые факторы, способствующие росту киберпреступности в условиях социально-политического кризиса.

Практическая значимость: результаты исследования имеют важное прикладное значение для совершенствования правовых, технологических, социальных и экономических механизмов противодействия киберпреступности в Камеруне. Предложенные рекомендации включают реформирование процессуального законодательства, расширение полномочий специализированных органов, введение системы домашних адресов и номеров социального страхования, повышение минимальной заработной платы и интеграцию курсов кибербезопасности в образовательные программы. Полученные данные могут быть использованы правительственными структурами, судебной системой, образовательными учреждениями и международными организациями для разработки эффективных стратегий борьбы с киберпреступностью и развития безопасной цифровой экономики.

Для цитирования

Лекунзе, А. Б. (2025). Влияние киберпреступности на электронную коммерцию в Камеруне: социально-правовые и экономические последствия. *Journal of Digital Technologies and Law*, *3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

Содержание

Введение

Преступления – частое явление в каждом человеческом обществе, они появились в древности и продолжают существовать до сих пор (Chris et al., 2005). После того как 1 января 1983 г.[1] был открыт публичный доступ в Интернет, стало возможным совершение преступлений с помощью коммуникационных порталов в Сети, что изначально не было предусмотрено законодателем. Первое в истории зафиксированное киберпреступление произошло в 1834 г., когда была взломана система телеграфа во Франции и с помощью украденных данных был получен доступ к финансовым рынкам[2]. В отличие от обычных преступлений акт совершения киберпреступления включает в себя различные элементы, инструменты и процессы, вызывающие проблемы с юрисдикцией и доказыванием. Это объясняется тем, что киберпространство обширно и не ограничено географическим регионом или страной (Yokotani & Takano, 2021; 2022).

Киберпреступность можно определить как широкий спектр преступных действий, которые осуществляются с использованием цифровых устройств и сетей (Alhadidi et al., 2024; Arroyabe et al., 2024; Edwards & Hollely, 2023; Gupta et al., 2025; Higgs & Flowerday, 2025a)[3], а также как совокупность преступных действий, которые включают преступления против компьютеров и компьютерных систем (Payne, 2020). Компьютер может быть объектом совершения преступления или мишенью. Киберпреступностью также может называться любая преступная деятельность, в ходе которой компьютер используется как инструмент или средство совершения иных преступлений, например, в форме киберкражи или других связанных с ней незаконных действий, направленных против личности и собственности (Garner, 1999). Данная статья посвящена влиянию киберпреступлений на операции электронной коммерции (e-commerce) в Камеруне, поскольку научных исследований о влиянии киберпреступлений на коммерцию в Камеруне недостаточно. Примеры киберпреступлений включают, в частности, хакерские атаки, киберпреследование, диффамацию, бомбардировку электронными письмами, подделку данных, салями-атаки [также «салями-слайсинг» – метод киберпреступления, при котором злоумышленник совершает серию незначительных действий или краж, которые в совокупности могут привести к серьезному ущербу или компрометации данных, ресурсов или активов. – Прим. переводчика], отказы в обслуживании, атаки вирусов и червей, кражи интернет-времени и т. д. Операции электронной коммерции, как следует из названия, осуществляются в киберпространстве посредством однорангового электронного обмена данными (electronic data interchange, EDI) (Garner, 1999) и могут сопровождаться преступлениями.

---

1 1 января 1983 г. считается официальным днем рождения Интернета. До этого различные компьютерные сети не имели стандартного способа взаимодействия друг с другом. Был разработан новый протокол связи под названием Протокол межсетевого взаимодействия (Transfer Control Protocol/ Internetwork Protocol, TCP/IP). Это позволило осуществить коммуникацию между различными типами компьютеров в разных сетях. 1 января 1983 г. ARPANET и сеть передачи данных Министерства обороны официально перешли на стандарт TCP/IP, что стало рождением Интернета. https://clck.ru/3QEh9u

2 Blue Voyant. https://clck.ru/3QEh97

3 Следует отметить, что киберпреступления чаще совершаются в сфере коммерческих операций, чем в других областях.

Электронная торговля может принимать формы онлайн-покупок, общения с мобильными приложениями посредством чатов, чат-ботов и голосовых помощников[4]. Выделяют такие типы взаимодействия, как «бизнес-бизнес» (B2B), «бизнес-клиент» (B2C), «клиент-клиент» (C2C) и «клиент-бизнес» (C2B). Это практика покупки и продажи товаров и услуг через онлайн-сервисы для потребителей в Интернете и один из способов ведения бизнеса компаниями и частными лицами с целью максимизации прибыли в короткие сроки при одновременном снижении как постоянных затрат на широкий спектр активов, так и транспортных расходов из центральных деловых районов[5].

Электронная торговля обладает рядом преимуществ, однако киберпреступления препятствуют бесперебойному функционированию электронной коммерции и приводят к потере прибыли и доверия деловых партнеров. В Камеруне предпринимаются усилия по борьбе с киберпреступлениями с помощью законодательства и технологий, но пока они не оказали существенного влияния на коммерческие операции из-за недостатка новых технологий, слабой системы управления цифровыми правами[6], а также из-за простоты обхода технологических мер, удобства и скорости совершения киберпреступлений. Кроме того, преступники получают выгоды и удовлетворение, обходя те самые технологии, которые предназначены для защиты от киберпреступлений в рамках операций электронной коммерции.

В последние годы в Камеруне наблюдается рост числа киберпреступлений и связанных с ними правонарушений в сфере коммерческих операций в связи с расширением распространения Интернета, низкой стоимостью приобретения электронных устройств, глобальным экономическим кризисом, карантином из-за пандемии COVID-19 и появлением многочисленных платформ социальных сетей. Киберпреступления стали популярны в Камеруне примерно в 2005 г., до вступления в силу в 2010 г. законов о киберпреступности и электронной торговле. Это можно продемонстрировать на примере более ранних судебных дел: The People v. Obi Roland[7], The People v. Nfang Macknight[8], The People v. Mbah Valery[9], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[10], The people of Cameroon & another v. Tita Njina Kevin Ndango[11]. Все они рассматривались до принятия в 2010 г. законов о киберпреступности и электронной торговле в Камеруне, хотя о некоторых

4 VentureBeat. (2025, March 15). How to prepare your products and brand for conversational commerce. https://clck.ru/3QEhWE

5 Это положение объясняет теория сельского хозяйства фон Тюнена, разработанная Иоганном Генрихом фон Тюненом в 1826 г. Эта модель предсказывает поведение человека с точки зрения ландшафта и экономики на основе тщательных математических расчетов и наблюдений. Она объясняет стоимость транспортировки от географического расположения фермы до центрального делового района города. Разработанная для сельского хозяйства, сегодня эта теория относится к электронной коммерции, поскольку основной целью электронной коммерции является минимизация транзакционных издержек от места происхождения товаров и услуг до места нахождения потребителя.

6 Речь идет о технических способах защиты данных с использованием паролей, криптографии и стеганографии.

7 CFIB/55C/2008(Unreported).

8 CFIB/76C/2009(Unreported).

9 CFIB/255/2010(Unreported).

10 (2014) 2 SLR.

11 (2010) CCLR 1-126

из этих дел стало известно позже. При этом можно заметить, что гражданские стороны этих процессов практически не присутствовали в суде, что вызвало всплеск киберпреступлений в Камеруне. Этот аспект мы затронем ниже в данной работе.

Первые законодательные акты о киберпреступлениях и электронной торговле в Камеруне были приняты в декабре 2010 г. после участившихся случаев киберпреступности в стране. Они в основном касались коммерческих операций с использованием онлайн-платформ, которые представляли собой мошенничество[12] под видом законных деловых операций[13]. Именно поэтому Закон о киберпреступности и Закон об электронной торговле в Камеруне были приняты в одном и том же году.

В данной статье рассматривается влияние киберпреступности на операции электронной коммерции в Камеруне. Наряду с Уголовным и Уголовно-процессуальным кодексами Камеруна правовую основу для расследования и судебного преследования за киберпреступления обеспечивает Закон о киберпреступности. Он предусматривает различные виды киберпреступлений, включая незаконный перехват данных, хакерские атаки, компьютерное мошенничество, преступления, связанные с детской порнографией, и т. д. Этот закон носит не только адъективный, но и процедурный характер, поскольку он устанавливает правила расследования и судебного преследования киберпреступлений в условиях международного сотрудничества.

С другой стороны, основы электронной торговли в Камеруне заложил Закон об электронной торговле от 2010 г.[14] Это произошло из-за стремительного развития платформ электронной коммерции в русле мировых тенденций. Закон также предусматривает все существенные элементы и процедуры для расследования и судебного преследования по искам о нарушениях в рамках электронных сделок.

Киберпреступления в Камеруне связаны не только с операциями электронной коммерции, но и с другими преступными деяниями, такими как диффамация, мошенничество, кражи, киберпреследование и хакерские атаки. Закон № 2010/012 от 21 декабря 2010 г. о кибербезопасности и киберпреступности в Камеруне предусматривает уголовную ответственность за киберпреступления, как и Закон № 2016/007 от 12 июля 2016 г. в Уголовном кодексе[15]. Закон № 2010/021 от 21 декабря 2010 г. об электронной торговле в Камеруне устанавливает правонарушения и наказания за нарушение положений правил электронной торговли. Влияние киберпреступности на электронную коммерцию в Камеруне огромно, учитывая тот факт, что большинство граждан страны не владеют компьютерной грамотностью и не могут позволить себе подключение к Интернету для изучения деятельности на электронных коммерческих площадках. Это приводит к ряду юридических

12 Закон № 2016/007 от 12.08.2016. Раздел 318.

13 Киберпреступность в Камеруне была официально признана как юридическая проблема в декабре 2010 г. с принятием Закона № 2010/012, который определяет киберпреступления и предусматривает наказание за них. До принятия этого закона многие случаи киберпреступности рассматривались в соответствии с Уголовным кодексом Камеруна.

14 Закон № 2010/021 от 21.12.2010.

15 Уголовный кодекс Камеруна. Раздел 219.

проблем, таких как злоупотребление доверием, потеря прибыли как на микро-, так и на макроэкономическом уровнях, рост взяточничества и коррупции и общий рост преступности, поскольку незаконные доходы, полученные в результате таких преступных деяний, часто используются для совершения новых преступлений.

1. Постановка проблемы

Внедрение электронной коммерции в Камеруне и распространение киберпреступности имели разрушительные последствия для бизнеса, основанного на цифровых технологиях. Ситуация усугубляется тем, что подавляющее большинство населения Камеруна получает зарплату ниже уровня минимальной заработной платы, а также в стране отсутствует система официальных домашних адресов и номеров социального страхования граждан. Отсутствие цифровых домашних адресов и номеров социального страхования затрудняет проведение расследований, выдачу повесток и арестов, поскольку доставка[16] обычно осуществляется в почтовых отделениях или в других местах по требованию, а платежи переводятся на банковские счета, которые не привязаны к конкретным адресам их владельцев. В настоящее время в Камеруне все чаще наблюдается потеря доверия к электронным коммерческим операциям, поскольку многие платежи являются необеспеченными[17]. Это приводит к огромным потерям прибыли и росту преступности по всей стране, поскольку незаконные доходы, полученные от киберпреступлений, часто используются для содействия совершению других преступлений, таких как злоупотребление наркотиками, взяточничество, коррупция, преступления против нравственности, пьянство в общественных местах и т. д. Киберпреступления также привели к широкому распространению произвольных, без наличия весомых доказательств, арестов и пыток, особенно в отношении молодежи, поскольку некоторые сотрудники полиции и судебных органов принимают на веру обвинения в мошенничестве из-за образа жизни даже без каких-либо официальных исков. Большинство из этих сотрудников практически не занимаются расследованием киберпреступлений в сфере электронной коммерции, а предпочитают обогащаться, получая взятки за освобождение подозреваемых. Это усугубляется тем фактом, что большинство жертв не подают официальных жалоб на преступников. В Камеруне также наблюдается низкий уровень международного сотрудничества в борьбе с киберпреступлениями, связанными с электронной коммерцией, из-за неадекватной технической инфраструктуры, личной финансовой выгоды и отсутствия надлежащего контроля. Это привело к росту числа таких киберпреступлений в стране, причем большинство правонарушителей предпочитают давать взятки и находят других жертв, чтобы возместить свои убытки[18]. Кроме того, существует общая атмосфера боязни подавать официальные жалобы на киберпреступников из-за позора и возможных тяжелых последствий, поскольку большинство

[16] Хотя для задержания подозреваемых в почтовых отделениях могут осуществляться контролируемые доставки, в Камеруне это почти не практикуется.

[17] Правила возврата денег в Камеруне крайне неэффективны и практически не закреплены в коммерческих контрактах. Таким образом, у клиентов возникают опасения.

[18] Можно заметить, что большинство киберпреступников в сфере электронной коммерции не прекращают свои действия даже после того, как обогатились. В основном они совершенствуют свои навыки.

жертв с самого начала являются сообщниками преступников в совершении незаконных операций. Все эти проблемы усугубились из-за отсутствия достаточных полномочий у таких ведомств, как Национальное агентство финансовых расследований (National Financial investigation agency, NFIA) и Национальное агентство информационно-коммуникационных технологий (National Agency for information and communication technologies, NAICT), для судебного преследования киберпреступлений в Камеруне. Их функции сводятся к подаче исков, проведению расследований и вынесению рекомендаций без надлежащего контроля.

2. Теоретические и концептуальные основы

Настоящее исследование базируется на ряде теоретических положений.

2.1. Теория утилитаризма

Данная теория была выдвинута Джоном Стюартом Миллем в 1861 г. Он считал, что счастье – это единственное, чего люди могут и должны желать ради самих себя. Теория гласит, что поскольку счастье – это единственное внутреннее благо и большее счастье предпочтительнее меньшего, то цель этической жизни – максимизировать счастье. Джереми Бентам и Джон Стюарт Милль назвали это положение «принципом полезности», или «принципом наибольшего счастья». В контексте нашего исследования киберпреступления в сфере электронной коммерции удовлетворяют потребности, обеспечивают благополучие и счастье преступников. Таким образом, стремление правонарушителей удовлетворить свое личное эго и обрести счастье побуждает их желать выгоды от обмана других людей путем совершения киберпреступлений в рамках электронной коммерции для получения удовольствия и удовлетворенности. Эта теория согласуется с теорией ресурсоемкой оценочно-максимизирующей модели (Resourceful Evaluative Maximizing Model theory), которая рассматривает индивидов как рациональных субъектов, всегда стремящихся максимизировать для себя пользу или благополучие в рамках заданного набора ограничений. Это показывает, что люди всегда стремятся найти наилучший возможный результат с учетом ограниченности своих ресурсов (Wartiovaara, 2011).

2.2. Теория транзакционных издержек

Эта теория была предложена Джоном Р. Коммонсом в 1931 г. (Williamson, 2008). Речь идет об издержках, возникающих в ходе торговли. Эти издержки связаны с управлением экономической системой компании и общими затратами на проведение транзакции. Сюда также входят затраты на планирование, принятие решений, изменение планов, разрешение споров и послепродажное обслуживание. По мнению автора теории, детерминантами операционных издержек являются частота, специфичность, неопределенность, ограниченная рациональность и оппортунистическое поведение. Одной из целей электронной коммерции является существенное снижение транзакционных издержек посредством электронного обмена данными (electronic data interchange, EDI). Теория транзакционных издержек (Transaction Cost Theory, TCT) изучает минимальные объемы ресурсов и затраты, необходимые сторонам для обмена товарами и услугами. Цель этой теории – максимизировать эффективность транзакций при минимизации затрат, что также является основной целью электронной

коммерции. Эту теорию можно сравнить с моделью фон Тунена, которая рассматривает транзакционные издержки, такие как перевозка урожая с ферм в центральный деловой район города. Цена продажи в основном определяется в зависимости от расстояния между центральным деловым районом и местом продажи сельскохозяйственной продукции. Эта теория связана с электронной коммерцией тем, что фокусируется на расстоянии между местами, где расположены товары и услуги, где проводятся переговоры о закупках и куда доставляются товары. Электронная коммерция в соответствии с этой моделью приводит к снижению затрат, независимо от того, где производятся товары и куда они доставляются, в отличие от обычных сделок, при которых сторонам приходится преодолевать большие расстояния для проведения переговоров и совершения покупок в реальном мире.

2.3. Теория рационального выбора

Эта теория была выдвинута Адамом Смитом в 1776 г. и позже сформулирована социологом Джорджем Хомансом в 1961 г. Она основана на поведенческой психологии и предполагает достижение цели с использованием наиболее экономичного метода, независимо от ценности этой цели. Цели могут быть корыстными, эгоистичными или материалистическими (Snidal, 2013). Теория дает рекомендации, которые помогают понять экономическое и социальное поведение и используются в криминологии. Это позволяет предсказать характер и результат выбора. Предполагается, что люди руководствуются личными интересами, а их решения основаны на оптимизации предпочтений путем балансирования затрат и выгод. Это явление распространено в электронной коммерции, где доступно множество вариантов онлайн-покупок и можно сделать свой выбор. Цели киберпреступников в сфере электронной коммерции обычно сосредоточены на них самих; они не заботятся о вреде, который причиняют своим жертвам, лишая их денежных средств. Эта теория также применима к случаям, когда человек принимает решение пойти на риск, чтобы совершить преступление и остаться на свободе, при этом получив выгоду. Это типичное явление в киберпреступлениях, связанных с электронной коммерцией, когда трудно поймать преступников на месте преступления.

3. Обзор научной литературы

Ряд авторов изучали области киберпреступности и электронной коммерции, не придавая особого значения связи между ними. Хотя некоторые авторы обращали внимание на влияние киберпреступности на операции электронной коммерции, они не исследовали критически взаимосвязь между ними, которая носит метафорический характер. Это объясняется тем, что те же санкции, которые применяются к обычным преступлениям в рамках коммерческих операций, применяются и к киберпреступлениям в рамках операций электронной коммерции. То, что происходит в реальном мире, ничем не отличается от того, что происходит в режиме онлайн, с той разницей, что в последнем случае для выполнения одного и того же действия используются определенные настройки и интерфейсы.

Reyns и соавторы (2011) подробно изучали опасения, вызываемые киберпреступлениями из-за виктимизации. Авторы исследуют взаимосвязь между риском в киберпространстве и страхом стать жертвой киберпреступности. Их анализ основан на информации, полученной от студентов Университета Цинциннати. Исследование

показало, что многие люди опасаются стать жертвами киберпреступлений. Авторы также выделяют категории правонарушителей и их поведенческие особенности в зависимости от статуса и пола. В работе рассматриваются особенности поведения, которые оказывают существенное влияние на уровень страха перед киберпреступностью. Авторы показывают, что страх и виктимизация в киберпространстве основаны на предполагаемых рисках. В работе не анализируются способы ослабить эти страхи, чтобы стимулировать электронную коммерцию.

Böhme и Moore (2012) описали киберпреступления в сфере онлайн-покупок и способы их предотвращения. Их основной вывод состоял в том, что киберпреступления приводят к снижению количества транзакций, таких как онлайн-банкинг и покупки онлайн, что имеет огромные негативные последствия. В работе показано, что люди, которые не знают о киберпреступлениях, с большей вероятностью совершают транзакции в рамках электронной коммерции, например, покупки онлайн. Исследование в основном посвящено онлайн-покупкам, в то время как понятие электронной коммерции гораздо шире.

В работе Y. Abubakari (2020) показано, что люди упускают множество возможностей из-за страха быть обманутыми. Автор пишет о причинах, последствиях и ограничениях политики в области киберпреступности в англоязычной Западной Африке. Он также демонстрирует, что киберпреступники теряют интерес к получению образования и что причина роста киберпреступлений связана с экономической напряженностью и коррупцией на правительственном уровне. Автор рассматривает препятствия в борьбе с киберпреступностью, такие как коррупция, вмешательство правительства, неэффективное применение законов о борьбе с киберпреступностью и непоследовательность соответствующих мер. Исследование фокусируется на Гане, Нигерии и странах Африки к югу от Сахары в качестве репрезентативной выборки для англоязычной Западной Африки, поскольку распространенность интернет-мошенничества в Западной Африке особенно высока в таких англоязычных странах, как Гана, Нигерия, Либерия, Сьерра-Леоне, Гамбия и часть Камеруна, достигает наибольших масштабов в Нигерии и Гане.

Исследование авторов Boraine и Leno Doris (2019) посвящено борьбе с киберпреступностью в Камеруне. Они сосредоточились главным образом на конфликте в англоязычных регионах страны и показали связь между этим конфликтом и ростом числа киберпреступлений. Были также проанализированы роль правительства Камеруна в борьбе с киберпреступлениями и некоторые правовые положения, используемые для борьбы с киберпреступлениями в стране. В работе рассматривались причины распространенности киберпреступлений и рекомендовались меры, которые могут быть приняты для борьбы с ними. Авторы не показали прямого влияния киберпреступлений на операции электронной коммерции. Исследование способствует углублению знаний о правилах защиты данных, особенно среди сотрудников следственных органов, студентов, специалистов и юристов-практиков.

Большая часть доступной литературы, рассмотренной выше, посвящена либо киберпреступности, либо электронной коммерции. В настоящей статье мы покажем непосредственное влияние киберпреступлений на операции электронной коммерции в Камеруне и дадим рекомендации по решению данной проблемы.

4. Распространенные типы киберпреступлений в сфере электронной коммерции в Камеруне

Киберпреступления в сфере электронной коммерции в Камеруне привели к потере примерно 12,2 млрд франков CFA в 2021 г., причем примерно половина этой суммы приходится на мошенничество и фишинг[19]. Существуют различные виды киберпреступлений, связанных с электронной коммерцией, которые затрагивают Камерун и весь мир. Очевидно, что характер коммуникаций в киберпространстве не ограничивает киберпреступления определенными географическими территориями. Человек может находиться в одной стране и совершать киберпреступления в разных странах с разными правовыми системами. Таким образом, существует необходимость в международном сотрудничестве для борьбы с киберпреступлениями, особенно с киберпреступлениями, связанными с электронной торговлей. По этой же причине истцы не обращаются в судебные инстанции, а число киберпреступлений растет[20]. Виды киберпреступлений, связанных с электронной коммерцией, включают, в частности: рассылку спама, салями-атаки, распространение вирусов, кибердиффамацию и т. д. Распространенными видами киберпреступлений в Камеруне являются мошенничество[21], фишинг[22] и хищения с банковских карт[23]. Большинство этих преступлений направлены на получение финансовой выгоды и совершаются в сфере электронной коммерции между отдельными гражданами.

4.1. Мошенничество

Мошенничество (scamming) – это получение денег или каких-либо преимуществ нечестным путем, особенно путем обмана. Такой обман может принимать большие масштабы. Мошенничество в Камеруне встречается относительно редко[24]. Этот термин также означает уловку, направленную на то, чтобы обмануть человека или группу людей, завоевать их доверие, воспользовавшись такими факторами, как наивность, сострадание, тщеславие, самоуверенность или жадность жертвы (Orbach & Huang, 2018). Согласно отчету Министерства почты и телекоммуникаций за 2021 г., уровень мошенничества в Камеруне составил 60 % в городах Яунде, Дуала, Буэа и Нун среди безработной молодежи в возрасте от 16 до 35 лет[25].

---

19 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 30. https://clck.ru/3QMjCH

20 Одной из причин нежелания преследовать киберпреступников в судебном порядке в Камеруне является то, что пострадавшие иногда являются гражданами других стран и их судебное преследование затруднено из-за ряда юридических сложностей, затрат и опасений. Это приводит к взяточничеству и коррупции, поскольку пострадавшие могут находиться в другой стране.

21 Обман с использованием протоколов электронной связи.

22 Преступник выдает себя за доверенное лицо, чтобы получить доступ к конфиденциальной информации.

23 Преступник получает данные банковской карты, когда ее владелец пользуется банкоматом.

24 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 6, с. 1346. https://clck.ru/3QMjCH

25 Там же.

Мошенничество – не новое явление, но оно усилилось с распространением ИКТ и Интернета. Еще в Древней Греции существовали наперсточники. Также в Греции «мошенник на доверии» по имени Томпсон выманивал деньги и был арестован в июле 1849 г.[26] Киберпреступления, связанные с электронной коммерцией, распространились в Камеруне в 2005 г., до вступления в силу Закона о кибербезопасности 2010 г. До этого суды при рассмотрении таких дел в основном полагались на Уголовный кодекс[27], как в деле The People v. Obi Roland[28]. Это дело о мошенничестве рассматривалось судом первой инстанции города Буэа в 2008 г., еще до вступления в силу законов о кибербезопасности и электронной коммерции 2010 г. В основу приговора была положена статья 318 Уголовного кодекса Камеруна. Обвиняемый был признан виновным и приговорен к шести годам тюремного заключения. В деле The People v. Nfang Macknight[29] тот же суд признал обвиняемого виновным по аналогичным основаниям.

Хотя суды часто выносят обвинительные приговоры, многие из таких дел в Камеруне не доходят до суда. Процедура рассмотрения дел о кибератаках часто изобилует несоответствиями, такими как нарушение прав, предусмотренных ст. 3 и 8 УПК, что привело к освобождению некоторых обвиняемых, как в делах The People v. Mbah Valery[30] и The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[31]. Можно заметить, что из-за высокого уровня взяточничества и коррупции в делах о киберпреступлениях, связанных с электронной коммерцией, таких как мошенничество, суды в Камеруне в настоящее время практически не рассматривают такие дела. Мошенники и следователи предпочитают вступать в сговор, давая и получая взятки в обмен на свободу. Однако это может оказаться затруднительным в ситуациях, когда истец решает продолжить судебное преследование, подав гражданский иск в соответствующий суд. Так было в деле The people of Cameroon & another v. Tita Njina Kevin Ndango (Jansson & von Solms, 2011), когда суд первой инстанции города Буэа признал обвиняемого виновным по всем пунктам обвинения, поскольку истец прибыл из Швейцарии для участия в слушании.

4.2. Фишинг

Это вид мошенничества, при котором жертв обманом заставляют раскрыть конфиденциальную информацию или устанавливают вредоносное ПО, которое совершает салями-атаки, содержит вирусы или программы-черви, которые отображают нужный веб-сайт (Jansson & von Solms, 2011). Например, в написание названия или адрес сайта вносятся небольшие изменения, чтобы он походил на оригинальный, так что жертва не подозревает, что имеет дело с поддельным веб-сайтом.

---

26 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 29. https://clck.ru/3QMjCH

27 Закон № 2016/007 от 12 июля 2016 г. в Уголовном кодексе Камеруна.

28 CFIB/55C/2008(Unreported).

29 CFIB/76C/2009(Unreported).

30 CFIB/255/2010(Unreported).

31 (2014) 2 SLR.

Фишинг широко используется в Камеруне в мобильных сетях, когда жертвам звонят или отправляют текстовые сообщения-приманки с мобильного телефона. Поддельные сообщения, как правило, ссылаются на ошибочные денежные переводы на мобильные счета жертв. Злоумышленник тем временем вводит номер телефона жертвы в компьютерное приложение оператора мобильной связи (APP). Затем злоумышленник обманом заставляет жертву подтвердить данные своей учетной записи мобильного телефона, введя свой пароль для возврата денег с обещанием вознаграждения. Если жертва запрашивает услугу «мобильные деньги» на свой счет и вводит свой пароль на своем устройстве, он одновременно передается в приложение злоумышленника, где тот получает доступ к снятию или переводу средств. Эта схема широко распространена в Камеруне, и почти все пользователи мобильных телефонов столкнулись с этим явлением, причем большинство попалось на уловку. Это не только порождает страх, но и создает искаженное представление об электронной коммерции, осуществляемой компаниями мобильной связи, как об одном из способов мошенничества. Некоторые дела такого рода успешно рассматривались в судах, поскольку можно было отследить номер злоумышленника, но иногда преступники проявляли достаточную сообразительность, регистрируя счета для снятия средств на имена разных физических лиц, которые находятся в разных географических точках.

4.3. Хищение средств с банковских карт

При этом способе хищения (skimming) на банкоматах или внутри них, а также в других точках продаж устанавливаются технологические устройства, с помощью которых злоумышленники могут записывать данные карты и копировать их[32]. Ту же тактику преступники используют для получения конфиденциальной информации с дебетовой или кредитной карты. Эти устройства собирают и хранят данные, которые мошенники впоследствии используют для совершения покупок или снятия средств в разное время[33]. Скимминг банковских карт не очень распространен в Камеруне из-за отсутствия необходимых технологических устройств, а также из-за того, что большинство банкоматов и точек продаж оснащены камерами видеонаблюдения и охраной. Однако скиммеры также могут физически украсть данные карты, если оставить ее в зоне доступа.

4.4. Социально-правовые последствия киберпреступности для электронной коммерции в Камеруне

Киберпреступность имеет множество негативных последствий для бизнеса и пользователей электронной коммерции, начиная от потери доверия и заканчивая банкротством предприятий и другими социальными проблемами в разных странах (Luu et al., 2025; Higgs & Flowerday, 2025b; Lee et al., 2023; Holt, 2022; Hornuf et al., 2025). Киберпреступления, связанные с электронной коммерцией, имеют социальные

32 Federal Bureau of Investigation. Skimming. https://clck.ru/3QEhzV

33 BrightBridge Credit Union. https://clck.ru/3QEi7p

и юридические последствия и порождают страх перед виктимизацией у потенциальных пользователей, готовых оплачивать товары и услуги через онлайн-платформы. Страх – это фактор, который влияет на физическое и психологическое состояние каждого человека. Это подрывает доверие и заставляет граждан задуматься о балансе издержек и выгод. В результате они отдают предпочтение наличным расчетам[34].

Распространение киберпреступлений в сфере электронной коммерции можно объяснить с точки зрения теорий утилитаризма и рационального выбора[35], согласно которым люди склонны занимать положение, обеспечивающее максимальное удовлетворение их потребностей, даже если это означает принятие иррациональных решений, которые иногда могут привести к достижению позитивной цели, не опасаясь последствий. Утилитаристская точка зрения рассматривает удовлетворение как фактор, который может перевесить рациональное поведение. Это объясняет, почему занимаются мошенничеством большинство молодых камерунцев в таких районах, как Молико и Бамбили, в городах Буэа и Баменда, соответственно. Киберпреступность в сфере электронной коммерции также быстро растет в англоязычных регионах Камеруна из-за текущего социально-политического конфликта. Эта ситуация еще более усугубляется высоким уровнем безработицы среди молодежи, низким уровнем минимальной заработной платы и общей шкалы оплаты труда в стране[36]. Многие молодые люди в этих районах Камеруна, особенно женщины, открывают поддельные интернет-магазины, якобы осуществляющие электронные коммерческие операции через платформы социальных сетей, чтобы скрыть незаконные источники своего дохода. В прошлом киберпреступления, связанные с электронной коммерцией, в основном совершались мужчинами, которые прибегали к обману, создавая в электронном виде редкие изображения несуществующих предметов и животных, чтобы привлечь внимание жертв.

Благодаря внедрению современной инфраструктуры ИКТ и легкому доступу к Интернету по доступным ценам в Камеруне мошенничество и фишинг в настоящее время распространены в большинстве густонаселенных городов. В период с января по апрель 2025 г. в районе Молико в Буэа автором был проведен опрос и получено 250 выборочных ответов от случайных участников. Было обнаружено, что по меньшей мере 60 % молодых людей в Молико вовлечены в киберпреступления, связанные с электронной коммерцией. Собранные данные также показали, что 10 % преступников – женщины, а 50 % – мужчины в возрасте от 16 до 35 лет. Также было отмечено, что большинство жертв проживали в Молико и преступники были знакомы со своими жертвами. Преступники не были знакомы лишь с несколькими жертвами, которые проживали в разных городах Камеруна и за рубежом.

Исследование также показало, что незаконные финансовые доходы, получаемые в результате этих киберпреступлений, значительно различаются по суммам: лишь немногие преступники зарабатывают огромные суммы почти регулярно, в то

---

34 Многие камерунцы предпочитают оплачивать товары наличными, чтобы их можно было увидеть и оценить. Именно по этой причине большинство жителей Камеруна пользуются наличными, несмотря на связанные с этим риски.

35 См. выше раздел «Теория рационального выбора».

36 Минимальная заработная плата в Камеруне на 46 939 франков CFA меньше, чем в соседних африканских странах.

время как некоторые едва зарабатывают на ежедневные карманные расходы. Деятельность злоумышленников в основном была связана с мошенничеством и фишингом. Опрос показал, что большинство молодых людей в Молико вовлекаются в эту деятельность из-за желания удовлетворить свое эго с помощью денег; другими мотивами являются конкуренция, давление со стороны сверстников, склад характера и незначительное число судебных преследований благодаря коррупции. Также был сделан вывод, что большинство преступников по-прежнему активно участвуют в киберпреступлениях в сфере электронной коммерции и при этом продолжают совершенствовать свои навыки.

Также было обнаружено, что многие молодые люди бросили школу, как отмечал Юшаву Абубакари в статье, опубликованной в 2020 г. (Abubakari, 2020).· При этом некоторые молодые люди, занимавшиеся киберпреступностью, платили другим из своих незаконных доходов за сдачу школьных экзаменов[37].

Оккультные практики[38] также широко распространены среди киберпреступников в Камеруне, что приводит к печальным последствиям, поскольку большинство молодых людей с низкими интеллектуальными способностями убеждены, что успех их незаконной деятельности зависит от таких практик. Это привело к нескольким смертельным случаям и появлению организованных банд мошенников, которые иногда совместно дают взятки, чтобы «выручить» своих коллег, попавших в беду. Оккультные практики распространяются и на другие социальные сферы, такие как гомосексуализм, лесбийские практики, инцест и другие сексуальные действия[39].

Все эти факторы, как отмечалось ранее, способствовали высокому уровню отсева из школ, тем самым повышая уровень неграмотности среди молодежи в Камеруне. В то же время правительство Камеруна, несмотря на это, продолжает вкладывать средства в образование молодежи, субсидируя начальное, среднее и высшее образование по всей стране.

4.5. Распространение иных типов преступлений в связи с киберпреступностью в сфере электронной коммерции

Незаконное обогащение в результате киберпреступлений в сфере электронной коммерции приводит к распространению других преступлений, таких как злоупотребление наркотиками, проституция, пьянство в общественных местах, выдача себя за другое лицо на экзаменах, сексуальные преступления, диффамация, насилие, коррупция, кража личных данных, нападение, нанесение побоев, неосторожное вождение и т. д. Неожиданное обогащение может привести к развитию психопатических наклонностей, особенно среди молодых людей, чья психика еще не сформирована. Это также было отмечено в ходе проведенного опроса.

---

37 Некоторые случаи выдачи себя за другое лицо были выявлены во время заседаний дисциплинарного совета руководством университетов, расположенных в Молико.

38 Оккультизм – это различные практики и верования, связанные с изучением манипулирования сверхъестественными силами. Эта сфера включает широкий спектр практик, включая гадание, магию, алхимию, астрологию и спиритизм.

39 Однако сегодня в Камеруне есть правозащитники, которые осуществляют деятельность, направленную на защиту прав лесбиянок, геев, бисексуалов, трансгендеров и квир-людей (ЛГБТК) (Международное общественное движение ЛГБТ признано экстремистским и запрещено на территории РФ).

4.5.1. Утрата доверия пользователей в сфере электронной коммерции

Сегодня в Камеруне часто можно увидеть молодых людей, которые ведут эпатажный образ жизни и ездят на автомобилях определенных марок, не имея никаких доказательств своих финансовых возможностей. Это напрямую связано с высоким уровнем киберпреступлений и коррупции в сфере электронной коммерции. Индекс коррупции в Камеруне, по данным организации Transparency international, в 2024 г. составил 26 пунктов из 100, что намного выше, чем в большинстве стран мира[40]. Это происходит, в частности, из-за киберпреступлений в сфере электронной коммерции и безответственного отношения к расследованию таких преступлений, что связано со взяточничеством и коррупцией в стране и не получает реакции на уровне Интерпола.

Закон о кибербезопасности 2010 г. устанавливает юрисдикцию и полномочия сотрудников следственных органов[41], которые должны соблюдать уголовно-процессуальные нормы, закрепленные в Уголовно-процессуальном кодексе 2005 г.[42] Но, к сожалению, большинство из этих сотрудников вступают в сговор с преступниками ради личной выгоды, и поэтому большинство дел о киберпреступлениях не доходят до надлежащего рассмотрения в суде[43]. Нередки случаи, когда сотрудники полиции и жандармерии арестовывают подозреваемого в киберпреступлении из-за его подозрительной финансовой деятельности даже без заявления, а затем сопровождают подозреваемого к банкоматам, чтобы забрать свою предполагаемую долю незаконно полученных денег. Такие полицейские заставляют подозреваемых переводить деньги с их мобильных счетов на их собственные телефоны, а затем отпускают. Часто можно увидеть, как сообщники подозреваемых дают взятки за освобождение одного из них, попавшего в беду. Некоторые киберпреступники включают в свой список сотрудников правоохранительных органов, которые защищают их от любых возможных неожиданностей. Подозреваемые, которые отказываются сотрудничать с полицией, чаще подвергаются необоснованным арестам и содержанию под стражей с применением пыток. В связи с этим возникает вопрос о надлежащей правовой процедуре и несоблюдении сотрудниками полиции нормы о запрете пыток, закрепленной в Международном пакте о гражданских и политических правах (МПГПП), Африканской хартии прав человека и народов (АХПЧН) и актах национального законодательства.

Все эти негативные аспекты в значительной степени подорвали доверие граждан страны как внутри страны, так и за рубежом. Из-за отсутствия доверия снижены возможности для осуществления законных операций в сфере электронной коммерции в Камеруне с иностранными гражданами. Можно отметить, что многие камерунцы, проживающие за рубежом, хорошо известны своими киберпреступлениями, а некоторые из них отбывают длительные тюремные сроки в зарубежных странах. Феномен сокрытия киберпреступлений за взятку наблюдается сегодня во многих африканских странах (Sarefo et al., 2023; Matias, 2025). Большинство сотрудников следственных органов предпочитают брать взятки, а не преследовать виновных в суде.

---

40 Transparency International. https://clck.ru/3QEjAB

41 Закон № 2010/012 от 21 декабря 2010 г. О кибербезопасности и киберпреступности в Камеруне. Раздел 52(1).

42 Закон № 2005 от 27 июля 2005 г. об Уголовном-процессуальном кодексе Камеруна. Разделы 59 и 60.

43 Чаще всего взятки вымогаются у подозреваемых с помощью силы и принуждения.

Потеря доверия к коммерческим операциям ощущается на уровне межличностных взаимоотношений, на уровне организаций и государства в целом (Wright & Kumar, 2023; Yi et al., 2024; Porcedda, 2023; Sarkar & Shukla, 2024; Tok et al., 2025; Onwuadiamu, 2025). Как отмечали Rainer Bohme и Tyler Moore (2012), большинство людей, пострадавших от киберпреступлений в коммерческих операциях онлайн, никогда больше не участвуют в них из-за страха стать жертвами, в то время как те, кто не знает о киберпреступлениях, с большей вероятностью будут участвовать в коммерческих операциях онлайн. Таким образом, такие киберпреступления отрицательно влияют на желание иностранных граждан заключать сделки с камерунцами в сфере электронной торговли в целом. Это связано с жителями не только Камеруна, но и соседних западноафриканских стран, о чем пишет Yushawu (Abubakari, 2020).

Камерун понес значительные финансовые потери из-за киберпреступлений в сфере электронной коммерции. Поскольку в киберпространстве существует большая свобода выбора[44], потенциальные участники сектора электронной коммерции предпочитают иметь дело с гражданами других стран. Предполагаемый ущерб экономике Камеруна, нанесенный киберпреступлениями в этой сфере в 2021 г., был обнародован Министерством почты и телекоммуникаций, которое является компетентным ведомством по вопросам связи в Камеруне. Согласно отчету министерства по данным ANTIC и ANIF[45], в 2021 г. из-за мошенничества и фишинга Камерун потерял около 12,2 млрд франков CFA.

4.5.2. Необоснованные аресты и задержания в связи с киберпреступностью в сфере электронной коммерции

Произвольные аресты и задержания по подозрению в киберпреступлениях в сфере электронной коммерции, без каких-либо жалоб в нарушение надлежащей правовой процедуры, стали частым явлением в крупных городах Северо-Западного и Юго-Западного регионов Камеруна, таких как Буэа, Баменда и Лимбе. В преамбуле конституции Камеруна[46] четко указано, что ни одно лицо не может быть арестовано или содержаться под стражей иначе, как в порядке, установленном законом. Законом, который определяет такие аресты в Камеруне, является Уголовно-процессуальный кодекс[47]. Вопреки конституционным и процессуальным положениям об аресте и содержании под стражей, большинство подозреваемых в киберпреступлениях подвергаются произвольным арестам без ордера и без соблюдения процедуры задержания на месте преступления[48], предусмотренной УПК. Это может быть связано с тем, что лица, проводящие такой арест, осознают, что они могут быстро получить доход за счет взяток, ряд киберпреступников готовы платить в обмен на свою свободу.

---

44 По определению Lawrence Lessig, это демократия в киберпространстве.

45 Отчет Министерства почты и телекоммуникаций Камеруна за 2021 г. Прим. 24 и 25.

46 Закон № 96-6 от 18 января 1996 г. (с изменениями) Камеруна.

47 Закон № 2005 от 27 июля 2005 г. об Уголовном-процессуальном кодексе Камеруна. Раздел 30

48 Там же. Раздел 31.

Надлежащая правовая процедура является фундаментальным аспектом судебного разбирательства, направленного на защиту гражданских прав. Ее нарушение может привести к аннулированию всего дела[49]. В делах The People v. Mbah Valery[50], The people of Cameroon v. Tamukum Fonjiyang Ferdinand & one other[51] суд первой инстанции города Буэа оправдал и освободил обвиняемых из-за нарушения ряда процессуальных аспектов уголовного судопроизводства, включая незаконные аресты и содержание под стражей. В последнем случае суд первой инстанции постановил, что, хотя личность обвиняемых вызывает сомнения, они должны предстать перед судом свободными людьми. Это произошло из-за серьезных процессуальных ошибок, которые нарушили положения разделов 3 и 8 Уголовно-процессуального кодекса. Это решение не было направлено на поощрение действий обвиняемых, но в значительной степени продемонстрировало важность защиты основных прав человека[52]. Подозреваемые не должны задерживаться силами правопорядка в нарушение их конституционных и юридических прав под предлогом обеспечения соблюдения закона. Большинство таких арестованных не только подвергаются пыткам, но и их финансовые ресурсы вымогаются путем принуждения. Это происходит под предлогом борьбы сотрудников полиции с киберпреступлениями в Камеруне.

Следует пресекать произвольные аресты и задержания без соблюдения надлежащей правовой процедуры, поскольку они нарушают основополагающие принципы гражданской свободы, закрепленные в большинстве международных конвенций и национальных законах. Статья 9 Международного пакта о гражданских и политических правах (МПГПП) 1966 г. запрещает произвольные аресты и задержания, в то время как статья 6 Африканской хартии прав человека и народностей (АХПЧН) 1987 г. гарантирует право на свободу и четко определяет, что лишение этой свободы должно осуществляться по причинам и на условиях, установленных законом. Эти правовые положения применяются в Камеруне в соответствии со ст. 45 Конституции 1996 г. в новой редакции[53].

Случаи незаконных арестов и задержаний в связи с киберпреступлениями в сфере электронной коммерции более распространены в Северо-Западном и Юго-Западном регионах Камеруна по сравнению с другими регионами страны (Abubakari, 2020). Отчасти это объясняется социально-политическим кризисом, охватившим оба региона (Boraine & Leno Doris, 2019). Этот кризис способствовал росту киберпреступлений, связанных с электронной коммерцией, в то время как сотрудники полиции, которые были направлены в эти регионы, воспользовались возможностью незаконно арестовывать и задерживать подозреваемых для получения личной выгоды под предлогом пресечения экономических преступлений. Это привело к откровенному пренебрежению правовыми нормами, гарантирующими гражданские свободы.

---

49 См. Уголовно-процессуальный кодекс Камеруна об абсолютной и относительной недействительности. Разделы 3 и 8. См. также решение Lord Denning по делу United Africa Company Limited (U.A.C) v. Macfoy.

50 CFIB/255/2010(Unreported).

51 (2014) 2 SLR.

52 См. Международный пакт о гражданских и политических правах (МПГПП) и Африканскую хартию прав человека и народов (АХПЧН).

53 Закон № 96-6 от 18 января 1996 г. о Конституции Камеруна. Статья 45.

4.6. Экономические последствия киберпреступности для электронной коммерции

Рост киберпреступлений в сфере электронной коммерции в Камеруне привел к финансовым потерям физических и юридических лиц и к снижению стимулов для участия в операциях электронной коммерции. Это объясняется тем, что страх, вызванный киберпреступлениями, оказывает большее влияние в киберпространстве, поскольку многие люди опасаются стать жертвами таких преступлений (Yokotani & Takano, 2021). Это отражается на спросе на операции электронной коммерции и может значительно снизить оборот и объем производства из-за потери капитала и прибыли в результате действий киберпреступников. Некоторые финансовые потери из-за киберпреступлений в этой сфере могут привести к банкротству. Например, как указано выше, сумма финансовых потерь от киберпреступлений в 2024 г. составила около 12,2 млрд франков CFA. Это оказывает огромное влияние на экономику, и, кроме того, незаконные финансовые доходы, полученные в результате киберпреступлений, связанных с электронной коммерцией, не облагаются налогом.

Все вышеперечисленное препятствует бесперебойному функционированию электронной коммерции в Камеруне. Одной из целей электронной коммерции является обеспечение быстрого оборота. В связи с распространением киберпреступлений в Камеруне возникает огромная проблема, поскольку спрос на услуги электронной торговли сокращается. Потеря доверия из-за киберпреступлений в сфере электронной коммерции также значительно подрывает экономику страны через такие последствия, как усиление инфляции[54], распространение отмывания денег и подделок валюты.

Заключение

В статье рассмотрено влияние киберпреступности на электронную торговлю в Камеруне. Автор отмечает, что большинство киберпреступлений в Камеруне направлено на поддельные транзакции в сфере электронной торговли. Было установлено, что росту числа таких киберпреступлений способствует ряд факторов: экономическая ситуация в Камеруне, легкий доступ к информационно-коммуникационным технологиям, конфликт в Юго-Западном и Северо-Западном регионах страны, стремление граждан вести эпатажный образ жизни. Все это имеет социально-правовые и экономические последствия, а также приводит к распространению других видов преступлений. Результаты проведенного опроса и отчеты Министерства почты и телекоммуникаций демонстрируют, что киберпреступления, связанные с операциями электронной коммерции, в ряде крупных городов Камеруна в основном совершаются молодежью. Ожидается, что число потенциальных правонарушителей в будущем увеличится. Было также обнаружено слабое влияние учреждений, отвечающих за борьбу с киберпреступлениями в стране. Полученные данные свидетельствуют о том, что киберпреступления в сфере электронной коммерции в Камеруне привели к утрате доверия граждан, произвольным арестам и задержаниям в нарушение ряда

[54] Можно заметить, что цены на основные товары в городе Буэа высоки по сравнению с другими городами Камеруна из-за незаконного обогащения, которым в Буэа пользуются в основном молодые люди – мошенники.

международных договоров, конституционных и уголовно-процессуальных положений. В работе отмечено, что большинство подозреваемых избегают судебного преследования, поскольку сотрудники полиции предпочитают брать взятки и отпускать подозреваемых на свободу. Исследование также показало, что указанные киберпреступления подорвали репутацию камерунцев в стране и за рубежом, и многие иностранные граждане отказываются вести с ними онлайн-бизнес. Это объясняется отсутствием надлежащей системы домашних адресов и номеров социального страхования у камерунцев.

Для решения выявленных проблем рекомендуется провести в Камеруне правовые, технологические, социальные и экономические реформы. Необходимо усовершенствовать действующее законодательство, уделив особое внимание процессуальным нормам на этапах расследования и судебного разбирательства по делам о киберпреступлениях, связанных с электронной коммерцией. Закон должен наделить Национальное агентство финансовых расследований (National Financial investigation agency, NFIA) и Национальное агентство информационно-коммуникационных технологий (National Agency for information and communication technologies, NAICT) полномочиями по судебному преследованию случаев киберпреступлений, связанных с электронной коммерцией. Силы правопорядка должны регулярно проходить обучение по вопросам ареста и задержания киберпреступников. Необходимо также предусмотреть стимулы для успешного расследования киберпреступлений, связанных с электронной коммерцией. В случаях коррупции и взяточничества в сфере киберпреступлений должны применяться серьезные санкции. Минимальный уровень заработной платы и шкала оплаты труда в Камеруне должны быть повышены при одновременном создании новых рабочих мест для неработающей молодежи. Следует включить уроки кибербезопасности и электронной коммерции в учебные программы, начиная с начальной школы и заканчивая университетами. В Камеруне необходимо ввести надлежащую систему домашних адресов и номеров социального страхования для идентификации граждан. Следует также усовершенствовать системы управления цифровыми правами и технологии отслеживания.

Список литературы

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Сведения об авторе

Лекунзе Анумбуандем Бенволио – PhD, преподаватель, кафедра английского права, Университет Буэа
Адрес: Камерун, г. Буэа, а/я 63
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

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: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 27 апреля 2025 г.
Дата одобрения после рецензирования – 9 мая 2025 г.
Дата принятия к опубликованию – 25 сентября 2025 г.
Дата онлайн-размещения – 30 сентября 2025 г.

Research article
UDC 34:004:343.721:004.8
EDN: https://elibrary.ru/tnqlxy
DOI: https://doi.org/10.21202/jdtl.2025.21

Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences

Anoumbuandem Benvolio Lekunze
University of Buea, Buea, Cameroon

Keywords

Cameroon,
cybercrime,
digital technologies,
e-commerce,
fraud,
justice,
law,
scamming,
security,
transactions

Abstract

Objective: to examine the impact of cybercrimes on e-commerce related transactions in Cameroon and evaluate the effectiveness of the legal provisions in force that counteract cyberthreats.

Methods: The research is based on the utilitarian, transaction cost and the rational choice theories. It adopts the qualitative research methodology with the use of the doctrinal method. The author conducted a comprehensive analysis of Cameroon's legal acts in the field of cybersecurity and e-commerce. A survey was carried out between January to April 2025 at Molyko in Buea where 250 sample responses were obtained. Judicial precedents and statistics of the Cameroon Ministry of Posts and Telecommunications were investigated.

Results: It was found that cybercrimes have caused loss of trust and confidence in e-commerce transactions within Cameroon and a declining rate at which people are willing to carry out e-commerce transactions in Cameroon. More than 60% of young persons between the ages of 16 to 35 years in some major Cameroonian cities are either involved in e-commerce related cybercrimes or suffered from them. It was also observed that there is an increase in the rate at which female persons are involved in e-commerce related cybercrimes. The main types of cybercrimes were identified: scamming, phishing, and bank card skimming.

Scientific novelty: it consists in a comprehensive interdisciplinary analysis of the impact of cybercrime on e-commerce in the context of the developing African economy. For the first time, an empirical study of the scale of cybercrime in a specific region of Cameroon was conducted, including

a quantitative assessment of youth involvement in illegal activities. The author has developed a theoretical model that combines the utilitarianism, transaction costs, and rational choice concepts to explain the motivation of cybercriminals. Specific socio-legal factors contributing to the growth of cybercrime in the context of the socio-political crisis were identified.

Practical significance: The study results are of great practical significance for improving the legal, technological, social and economic mechanisms for countering cybercrime in Cameroon. The proposed recommendations include reforming procedural legislation, expanding the powers of specialized agencies, introducing a system of home addresses and social security numbers, raising the minimum wage, and integrating courses on cybersecurity into educational programs. The data obtained can be used by government agencies, the judicial system, educational institutions and international organizations to develop effective strategies to combat cybercrime and develop a secure digital economy.

For citation

Lekunze, A. B. (2025). Impact of Cybercrime Related Offences on E-commerce in Cameroon: Social-Legal and Economic Consequences. *Journal of Digital Technologies and Law, 3*(3), 512–536. https://doi.org/10.21202/jdtl.2025.21

References

Abubakari, Y. (2020). The reasons, impacts and limitations of cybercrime policies in Anglophone West Africa: A review. *Social Space Journal*, *12*(3), 45–67.

Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of Cybercrime and legal awareness on the behavior of university of Jordan students. *Heliyon*, *10*(12), e32371. https://doi.org/10.1016/j.heliyon.2024.e32371

Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & De Arroyabe, J. C. F. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security*, *141*, 103826. https://doi.org/10.1016/j.cose.2024.103826

Böhme, R., & Moore, T. (2012). The market for stolen data: Estimating the costs of data breaches. *IEEE Security & Privacy*, *10*(2), 43–49. https://doi.org/10.1109/MSP.2012.40

Boraine, P. A., & Leno Doris, D. N. (2019). The Fight against Cybercrime in Cameroon. *International Journal of Computer (IJC)*, *35*(1), 87–100. https://doi.org/10.53896/ijc.v35i1.1469

Chris, H. et al. (2005). *Criminology*. Oxford: Oxford University Press.

Edwards, M., & Hollely, N. M. (2023). Online sextortion: Characteristics of offences from a decade of community reporting. *Journal of Economic Criminology*, *2*, 100038. https://doi.org/10.1016/j.jeconc.2023.100038

Garner, B. A. (1999). *Black's Law Dictionary* (7th ed.). Minnesota, West Group.

Gupta, A., Matta, P., & Pant, B. (2025). Analyzing the social conduct of users to detect and prevent cybercrime across social networks. *Procedia Computer Science*, *258*, 4269–4278. https://doi.org/10.1016/j.procs.2025.04.676

Higgs, J., & Flowerday, S. (2025a). Detecting cybercrime in online video gaming. *Computers & Security*, *156*, 104528. https://doi.org/10.1016/j.cose.2025.104528

Higgs, J., & Flowerday, S. (2025b). Cybercrime and virtual laundering in video game marketplaces: A Bayesian P-inductive argument. *Technology in Society*, *83*, 102978. https://doi.org/10.1016/j.techsoc.2025.102978

Holt, T. J. (2022). Understanding the state of criminological scholarship on cybercrimes. *Computers in Human Behavior*, *139*, 107493. https://doi.org/10.1016/j.chb.2022.107493

Hornuf, L., Momtaz, P. P., Nam, R. J., & Yuan, Y. (2025). Cybercrime on the ethereum blockchain. *Journal of Banking & Finance*, *175*, *107419*. https://doi.org/10.1016/j.jbankfin.2025.107419

Jansson, K., & von Solms, R. (2011). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929x.2011.632650

Lee, S., Kang, I., & Kim, H. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences*, *244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Matias, C. F. F. (2025). Access revisited: AI training at the intersection of copyright and cybercrime laws. *Computer Law & Security Review*, *57*, 106149. https://doi.org/10.1016/j.clsr.2025.106149

Onwuadiamu, G. (2025). Cybercrime in Criminology; A Systematic Review of criminological theories, methods, and concepts. *Journal of Economic Criminology*, *8*, 100136. https://doi.org/10.1016/j.jeconc.2025.100136

Orbach, B., & Huang, L. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, *85*(4), 795–822. https://doi.org/10.1353/sor.2018.0050

Payne, B. K. (2020). *The Handbook of International Cybercrime and Cyberdevidence*. London: Palgrave Macmillian. https://doi.org/10.1007/978-3-319-78440-3

Porcedda, M. G. (2023). Sentencing data-driven cybercrime. How data crime with cascading effects is tackled by UK courts. *Computer Law & Security Review*, *48*, 105793. https://doi.org/10.1016/j.clsr.2023.105793

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying Cyberlifestyle–Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Sarefo, S., Mphago, B., & Dawson, M. (2023). An analysis of Botswana's cybercrime legislation. *Procedia Computer Science*, *219*, 1023–1033. https://doi.org/10.1016/j.procs.2023.01.380

Sarkar, G., & Shukla, S. K. (2024). Reconceptualizing online offenses: A framework for distinguishing cybercrime, cyberattacks, and cyberterrorism in the Indian legal context. *Journal of Economic Criminology*, *4*, 100063. https://doi.org/10.1016/j.jeconc.2024.100063

Snidal, D. (2013). Rational Choice and Interntional Relations. In *Handbook of International Relations*. London, Sage. https://doi.org/10.4135/9781446247587.n4

Tok, Y. C., Zheng, D. Y., & Chattopadhyay, S. (2025). A Smart City Infrastructure ontology for threats, cybercrime, and digital forensic investigation. *Forensic Science International Digital Investigation*, *52*, 301883. https://doi.org/10.1016/j.fsidi.2025.301883

Wartiovaara, M. (2011). Rationality, REMM, and Individual Value Creation. *Journal of business Ethics*, *98*(4), 641–648. https://doi.org/10.1007/s10551-010-0643-6

Williamson, O. E. (2008). Outsourcing: Transaction Cost Economics and Supply Chain Management. *Journal of Supply Chain Management*, *44*, 2–82. https://doi.org/10.1111/j.1745-493x.2008.00051.x

Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts*, *1*(1–2), 100013. https://doi.org/10.1016/j.socimp.2023.100013

Yi, M., Li, J., & Shen, G. (2024). Can targeted poverty alleviation reduce criminal offenses? Empirical evidence from China judgments online data. *China Economic Quarterly International*, *4*(1), 55–68. https://doi.org/10.1016/j.ceqi.2024.03.003

Yokotani, K., & Takano, M. (2021). Predicting cyber offenders and victims and their offense and damage time from routine chat times and online social network activities. *Computers in Human Behavior*, *128*, 107099. https://doi.org/10.1016/j.chb.2021.107099

Yokotani, K., & Takano, M. (2022). Effects of suspensions on offences and damage of suspended offenders and their peers on an online chat platform. *Telematics and Informatics*, *68*, 101776. https://doi.org/10.1016/j.tele.2022.101776

Author information

Anoumbuandem B. Lekunze – PhD, Lecturer, Department of English Law, University of Buea
Address: PO Box 63, Buea, Cameroon
E-mail: benleku@yahoo.com
ORCID ID: https://orcid.org/0009-0005-9947-0639

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 – April 27, 2025
Date of approval – May 9, 2025
Date of acceptance – September 25, 2025
Date of online placement – September 30, 2025