ISSN 2949-2483

Volume 3 Number 1

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

2025

ELECTRONIC SCIENTIFIC AND PRACTICAL JOURNAL

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW

Том 3, № 1
2025
DOI: 10.21202/2949-2483.2025.1

ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

eISSN 2949-2483

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

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 марта 2025 г. Дата онлайн-размещения на сайте https://www.lawjournal.digital – 30 марта 2025 г.

JOURNAL OF DIGITAL TECHNOLOGIES AND LAW
Том 3, № 1
2025
DOI: 10.21202/2949-2483.2025.1
ЭЛЕКТРОННЫЙ НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ
eISSN 2949-2483

Содержание

Научная статья
УДК 34:004:347.6:004.9:004.056
EDN: https://elibrary.ru/eaqyqj
DOI: https://doi.org/10.21202/jdtl.2025.1

Цифровая трансформация системы регистрации актов гражданского состояния Камеруна: инновации в электронном управлении

Роберт Кошо Ндиюн ✉

Технологический университет Тшване, Претория, ЮАР

Рикки Муньярадзи Муконза

Технологический университет Тшване, Претория, ЮАР

Ключевые слова

акт гражданского состояния,
государственная услуга,
законодательство,
защита данных,
Камерун,
право,
цифровая грамотность,
цифровые технологии,
электронное правительство,
электронное управление

Аннотация

Цель: исследование инновационных преобразований в сфере электронного управления, внедренных в систему регистрации актов гражданского состояния Камеруна в результате законодательных реформ 2024 года. Основное внимание уделяется оценке влияния этих преобразований на повышение эффективности управления, прозрачности, доступности услуг для граждан, а также на совершенствование статистического учета жизненно важных событий.

Методы: в работе использованы общенаучные методы анализа и синтеза, классификации, системный и функциональный подходы, а также формально-юридический и сравнительно-правовой методы.

Результаты: внедрение электронного декларирования актов гражданского состояния, создание Национальной базы данных и переход на электронные свидетельства способны существенно повысить эффективность и доступность услуг для населения. Однако авторы подчеркивают, что успешная реализация цифровых инноваций требует преодоления значительных барьеров, таких как недостаточная технологическая оснащенность, ограниченный доступ к Интернету и низкий уровень цифровой грамотности среди граждан. Эти вызовы делают необходимой разработку дополнительных механизмов регулирования и поддержки. Особое значение придается балансу между цифровизацией и обеспечением прав граждан в контексте электронной регистрации.

✉ Контактное лицо

Научная новизна: заключается в предоставлении уникальных эмпирических данных о процессе цифровизации государственных услуг в Камеруне, что особенно актуально для стран глобального Юга, где подобные преобразования происходят медленно и фрагментарно. Исследование вносит значительный вклад в научную дискуссию, расширяя понимание моделей внедрения цифровых технологий через призму ожидаемой полезности и воспринимаемой простоты использования в условиях развивающихся стран.

Практическая значимость: состоит в разработке конкретных рекомендаций для законодателей, государственных служащих и других заинтересованных сторон. Авторы подчеркивают необходимость скорейшего принятия нормативной правовой базы, внедрения образовательных программ для сотрудников и граждан, а также обеспечения доступа к цифровым технологиям. Эти меры направлены на создание устойчивой инфраструктуры для эффективного перехода к электронным системам и повышение качества государственных услуг. Работа представляет собой важный вклад в изучение процессов цифровизации государственного управления, предлагая как теоретические выкладки, так и практические решения, которые могут быть адаптированы для других стран с аналогичными вызовами.

Для цитирования

Ндиюн, Р. К., Муконза, Р. М. (2025). Цифровая трансформация системы регистрации актов гражданского состояния Камеруна: инновации в электронном управлении. *Journal of Digital Technologies and Law*, *3*(1), 7–34. https://doi.org/10.21202/jdtl.2025.1

Содержание

Введение

Важность информационно-коммуникационных технологий для повышения эффективности управления и предоставления услуг становится центральной в современном, все более взаимосвязанном мире. Государства стремятся повышать эффективность и прозрачность своей деятельности, и внедрение механизмов электронного управления (e-governance) стало важным инструментом преобразования государственного управления (Bannister & Connolly, 2012; Oliveira et al., 2020). Степень внедрения этих инструментов различна. По данным Организации Объединенных Наций, 161 страна предлагает онлайн-платформы для подачи заявлений на получение свидетельств о рождении, 152 страны предоставляют цифровые услуги для получения свидетельств о браке, а 151 страна предлагает электронные услуги для подачи заявлений на получение свидетельств о смерти, что соответственно на 3, 1 и 8 % больше, чем в 2022 г. соответственно[1]. Такой рост компьютеризации в сфере декларирования и регистрации актов гражданского состояния отражает важность этих систем для государственного управления. В то время как в большинстве стран глобального Севера эти услуги полностью переведены в цифровую форму, на глобальном Юге ситуация обратная, особенно в Африке, где уровень полной цифровизации заявлений на получение свидетельств о рождении составляет 11 %, а на выдачу свидетельств о браке и смерти – 7 %[2]. В Камеруне государственный сектор находится в процессе перехода на электронное предоставление услуг[3]. Это предусмотрено Национальным стратегическим планом развития информационно-коммуникационных услуг (далее – ИКТ) на период с 2016 по 2020 г. и Национальной стратегией развития до 2030 г., которые отводят основную роль цифровизации государственного управления для достижения целей устойчивого развития и превращения Камеруна в страну с формирующейся экономикой к 2035 г. (Sevidzem, 2024).

Непрерывное развитие технологий отвечает потребностям граждан, поэтому государство должно обеспечивать предоставление услуг с использованием ИКТ. В настоящей статье рассмотрены электронные инновации, предусмотренные Законом № 2024/016 от 23 декабря 2024 г. для внедрения в системы регистрации актов гражданского состояния в Камеруне. Данный закон соответствует вышеупомянутым политическим документам, которые предполагают цифровизацию актов гражданского состояния и обеспечение перехода на цифровые технологии посредством соответствующих установлений и инструментов ИКТ во всех государственных учреждениях (Sevidzem, 2024). Эти инновации направлены на область регистрации актов гражданского состояния как необходимого инструмента, призванного укрепить гражданские права и организацию общества. Возможность корректно и эффективно регистрировать такие важные события, как рождение, брак и смерть, имеет основополагающее значение для целей национальной идентичности и социальной справедливости[4].

1 United Nations. (2024). E-Government Survey, 2024. UN (2020). https://clck.ru/3Gf8Ki

2 Там же.

3 Sindeu, E. (2013). Implementation of e-government in Cameroon. In 7th Annual E-Government Forum, Muyuno, Uganda, 25–27 March (pp. 1–24).

4 World Economic Forum. (2022, October 22). Civil registrations and vital statistics: Here's why they're fundamental to society. https://clck.ru/3Gf8Qt

Кроме того, гражданский статус имеет решающее значение для установления юридической идентичности граждан, гарантирования осуществления их прав и содействия их участию в социальной и политической жизни страны[5].

Необходимость совершенствования системы регистрации актов гражданского состояния (далее – АГС) в Камеруне стала особенно острой в последнее время. Система регистрации АГС в стране исторически сталкивалась с многочисленными препятствиями, включая неэффективность бюрократии, ограниченный доступ к услугам, недостаточную осведомленность общественности и низкий уровень регистрации рождений. В результате более семи миллионов граждан в настоящее время не имеют свидетельств о рождении[6]. После обретения независимости и воссоединения в Камеруне был принят Закон № 68-LF-2 от 11 июня 1968 г., регулирующий систему регистрации актов гражданского состояния. Этот закон был затем заменен Постановлением № 81-02 от 29 июня 1981 г. и позднее изменен Законом № 2011/011 от 6 мая 2011 г. Предусмотренное Законом 2011 г. Национальное бюро записи актов гражданского состояния (National Civil Status Bureau, BUNEC) было создано только в 2013 г. Указом Президента об организации и функционировании этой структуры[7]. Это учреждение, отвечающее за надзор, контроль, регулирование и оценку национальной системы регистрации актов гражданского состояния, начало функционировать только в 2016 г., а к 2023 г. представило официальный полный отчет о ситуации с АГС в Камеруне[8].

Процесс преобразования системы регистрации актов гражданского состояния в Камеруне был начат в 2007 г. в рамках Программы восстановления гражданского состояния (PRE2C). В 2010 г. Камерун присоединился к Африканской программе по ускоренному совершенствованию системы регистрации АГС и статистики естественного движения населения (APAI-CRVS), а позднее принял Стратегический план восстановления гражданского состояния на 2018–2022 гг. В 2015 г. распоряжением премьер-министра № 019/CAB/PM от 24 февраля 2015 г. был создан руководящий комитет для обеспечения PRE2C под председательством министра децентрализации и местного развития[9]. За этим последовало принятие генерального плана по компьютеризации национальной системы регистрации актов гражданского состояния на период 2019–2023 гг. Эти мероприятия способствовали принятию в 2024 г. Закона о системах регистрации актов гражданского состояния в Камеруне.

Система регистрации АГС в Камеруне является полудецентрализованной: существуют местные центры регистрации актов гражданского состояния и BUNEC на центральном уровне. Первые включают первичные центры регистрации актов

5 National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

6 Ayang, M. (2024, November 29). Cameroon introduces draft laws on civil registration reform, data protection. Biometric Updates. https://clck.ru/3Gf8ZM

7 National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

8 Там же.

9 Zewoldi, Y. (2019). Snapshot of Civil Registration and Vital Statistics in Cameroon. Centre of Excellence for Civil Registration and Vital Statistics. https://clck.ru/3Gf8q5

гражданского состояния на уровне местных советов и вспомогательные центры регистрации АГС в сельских поселениях и районах. В настоящее время в Камеруне насчитывается 375 основных центров регистрации актов гражданского состояния, 56 консульских учреждений и дипломатических миссий, а также 2455 вспомогательных центров[10]. Регистрация актов гражданского состояния в этих центрах осуществляется органами записи актов гражданского состояния – мэрами городов и их заместителями, главами поселений и их заместителями, которым помогают секретари (Постановление № 81-02, ст. 7).

Несмотря на эти меры, процесс декларирования и регистрации рождений и смертей в Камеруне затруднен из-за недостаточной осведомленности о важности свидетельств о гражданском состоянии, незнания правовых норм, регулирующих гражданский статус, финансовых трудностей, низкой доступности центров для населения, проживающего в анклавах, и административных проблем[11]. Принятие Закона 2024 г. знаменует собой фундаментальное новшество в решении этих проблем путем внедрения электронных систем, созданных для модернизации процессов и расширения участия граждан. Этот закон отражает стремление к преобразованию государственного управления и повышению общего качества управления в Камеруне[12]. К 2018 г. уровень регистрации рождений в Камеруне составлял 54 % от общего числа родившихся, в то время как число зарегистрированных смертей в 2020 г. составило 9,71 % от общего числа смертей[13].

Несмотря на то, что количество исследований, посвященных электронному управлению и его влиянию на различные сферы, растет, лишь немногие из них сосредоточиваются на электронных инновациях в области регистрации актов гражданского состояния в Камеруне, введенных Законом 2024 г. Существующие исследования по электронному управлению в Камеруне были посвящены процедурам налогообложения (Djossa-Tchokoté et al., 2024), предоставлению государственных услуг на местном уровне (Sevidzem, 2024), электронному участию в государственном управлении (Xin et al., 2023), общим вопросам внедрения электронного управления[14].

Наша статья призвана восполнить этот пробел путем критического изучения инноваций в области электронного управления, введенных Законом 2024 г., и их потенциала для реформирования системы регистрации актов гражданского состояния в Камеруне.

---

10 National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

11 Там же.

12 Ayang, M. (2024, November 29). Cameroon introduces draft laws on civil registration reform, data protection. Biometric Updates. https://clck.ru/3Gf8ZM

13 National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

14 Sindeu, E. (2013). Implementation of e-government in Cameroon. In 7th Annual E-Government Forum, Muyuno, Uganda, 25–27 March (pp. 1–24).

Главная проблема исследования заключается в следующем: как инновации в электронном управлении регистрацией АГС могут повысить административную эффективность и вовлеченность граждан в Камеруне? Чтобы решить эту проблему, в работе ставятся следующие исследовательские вопросы: (1) какие ключевые электронные инновации были введены Законом о регистрации актов гражданского состояния в Камеруне 2024 г.? (2) Как эти инновации влияют на предоставление услуг и управление в секторе регистрации актов гражданского состояния? (3) С какими проблемами и возможностями сталкиваются заинтересованные стороны при внедрении инновационной системы?

Целью данной статьи является: (1) изучение конкретных электронных инноваций, введенных Законом 2024 г., (2) оценка их последствий для предоставления услуг и управления и (3) выявление барьеров, с которыми заинтересованные стороны могут столкнуться при внедрении, и предложение стратегий для их преодоления.

Результаты исследования показывают, что создание Национальной базы данных о гражданском состоянии и внедрение электронных деклараций могут значительно повысить эффективность и доступность услуг по регистрации актов гражданского состояния[15]. Однако для реализации всего потенциала этих инноваций необходимо решить такие проблемы, как недостаточность технологической инфраструктуры и сопротивление общества изменениям.

Данная статья структурирована следующим образом. В первом разделе представлен всесторонний обзор литературы, выделены основные темы и пробелы, связанные с темой, а затем дается их теоретическое обоснование. В разделе «Методология» представлены дизайн исследования и методы сбора данных, использованные в работе. В разделе «Выводы» подробно описываются результаты анализа, затем следует обсуждение, в котором результаты рассматриваются в контексте более широкого применения электронного управления. В Заключении содержатся рекомендации по улучшению внедрения и повышению эффективности регистрации актов гражданского состояния в Камеруне.

1. Обзор литературы

1.1. Концепция электронного управления

Переход к электронному управлению знаменует собой преобразующий этап, на котором информационно-коммуникационные технологии используются для повышения эффективности предоставления государственных услуг. Он охватывает все аспекты деятельности правительства, связанные с ИКТ, включая предоставление услуг, участие граждан и управление данными для обеспечения подотчетности, эффективности и прозрачности политических процессов (Grigalashvili, 2022; Heeks, 2006). Это определение согласуется с мнением Umbach & Tkalec (2022) о том, что оно предполагает применение цифровых технологий для улучшения предоставления государственных услуг гражданам. Кроме того, электронное управление рассматривается как двусторонняя коммуникация между правительством и его внутренними

[15] Ayang, M. (2024, November 29). Cameroon introduces draft laws on civil registration reform, data protection. Biometric Updates. https://clck.ru/3Gf8ZM

и внешними заинтересованными сторонами, использующими цифровые инструменты[16]. Электронное управление выходит за рамки простой цифровизации сферы услуг; оно направлено на повышение оперативности и подотчетности государственных служб за счет улучшения коммуникации между населением и государственными учреждениями в режиме реального времени (Heeks, 2006). Эта революционная инновация особенно важна в сфере регистрации актов гражданского состояния, где внедрение технологий может рационализировать традиционную и существующую в настоящее время неповоротливую бюрократическую систему. Эффективное электронное управление требует надежной технологической инфраструктуры и надлежащего планирования для создания системы, которая была бы в большей степени ориентирована на интересы граждан.

Ряд ученых (Palvia & Sharma, 2007) не видят разницы между электронным правительством и электронным управлением. Однако Grigalashvili (2022) утверждает, что, хотя эти концепции и процессы направлены на улучшение взаимодействия правительства и пользователей с помощью цифровых технологий, первое является существенным компонентом второго. Электронное управление направлено на повышение эффективности работы правительства за счет улучшения обмена информацией и выработки политики между правительством и населением с использованием инструментов ИКТ. Облегчая обмен информацией для достижения политических целей (Muttoo et al., 2019), электронное управление создает информированное сообщество, сокращая временные интервалы вмешательства государства и улучшая предоставление услуг и участие общественности в цифровом процессе (Umbach & Tkalec, 2022).

Некоторые страны успешно применяют инновации в области электронного управления при регистрации актов гражданского состояния. Например, система электронного гражданства Эстонии получила высокую оценку как модель цифрового управления, предоставляющая резидентам и гражданам защищенный доступ к различным государственным услугам онлайн, включая регистрацию актов гражданского состояния (Tammpuu & Masso, 2018; Kattel & Mergel, 2019). Аналогичным образом, индийский подход Digital India направлен на повышение удобства использования услуг по регистрации актов гражданского состояния с помощью мобильных приложений и онлайн-систем (Suthar et al., 2019). Эти примеры демонстрируют, что успешное применение электронного управления часто требует твердой приверженности заинтересованных сторон, эффективной технологической настройки и решимости постоянно совершенствоваться. Прогресс в системах электронного управления свидетельствует о переходе к подходу к управлению, основанному на участии граждан, который расширяет их возможности. Однако инновации в области управления должны включать в себя как технический прогресс, так и социально ориентированные подходы. Эффективность инноваций в области электронного управления в значительной степени зависит от местных особенностей, таких как доступные технологические возможности, доверие общественности к правительству и существующие правовые механизмы (Suthar et al., 2019).

[16] Oyedokun, G., Adeolu-Akande, M., & Oyedokun, D. (2022). Assessing the Status and Challenges of e-Governance and e-Public Services Delivery in Nigeria. BAM 2022 Conference, University of Manchester (pp. 1–15).

1.2. Подходы к электронному управлению и области его применения

Учеными были предложены различные модели электронного управления, описывающие перемещение данных и услуг между поставщиком услуг (правительством) и пользователями (гражданами) (Grigalashvili, 2022; Halachmi, 2004; Prashar & Bawa, 2023). Эти подходы включают информационную поддержку в сфере электронных технологий, модель критического потока и сравнительный анализ (Prashar & Bawa, 2023). Модель критического потока предполагает быструю передачу жизненно важной информации целевым получателям с помощью ИКТ. Модель сравнительного анализа сосредоточена на поиске лучших практик в области электронного управления и применении их в качестве ориентиров для тестирования других систем управления (Halachmi, 2004; Grigalashvili, 2022). Модель информационной поддержки делает упор на усиление влияния различных сфер общественной жизни на политику правительства посредством их вклада и обратной связи (Albert, 2009). Потенциал модели критического потока заключается в использовании ИКТ для обеспечения мгновенной передачи информации, сокращения расстояний и времени. С другой стороны, модель сравнительного анализа опирается на неограниченные возможности электронных систем хранить ценную информацию, а также мгновенно извлекать и распространять ее, преодолевая многочисленные барьеры (Halachmi, 2004). Модель информационной поддержки как один из широко используемых подходов к цифровому управлению способна устранить институциональные и физические препятствия, мобилизовать человеческие ресурсы и информацию и применить их для конкретных действий.

Исследователи выделяют различные типы или области электронного правительства и электронного управления, основываясь на особенностях цифровых взаимодействий между правительством, гражданами, экономическим сектором, служащими и другими некоммерческими, политическими и социальными институтами (Fang, 2002). Отмечены следующие категории двустороннего цифрового взаимодействия: взаимодействие правительства с правительством (G2G); взаимодействие правительства с бизнесом (G2B); взаимодействие правительства с гражданами (G2C); взаимодействие правительства со служащими (G2E); и взаимодействие правительства с некоммерческими организациями (G2N) (Fang, 2002; Kaisara & Pather, 2011). G2G предполагает цифровое сотрудничество, коммуникацию, предоставление информации и товаров между правительственными ведомствами и агентствами для повышения эффективности работы правительства и эффективной координации мер. G2B фокусируется на цифровых коммуникациях между правительствами и предприятиями, включая электронные закупки, регистрацию бизнеса и финансовые операции. G2C состоит в создании электронных государственных услуг правительством для обеспечения доступа граждан. G2E касается того, как правительства реализуют инициативы, способствующие внутреннему обмену информацией между государственными служащими в целях цифровизации систем обработки и управления государственными услугами. Наконец, G2N предполагает информационную коммуникацию и транзакции между правительством и некоммерческими организациями, политическими партиями и другими социальными группами.

1.3. Значение и актуальность электронного управления

Внедрение различных типов электронного управления, рассмотренных выше, дает множество преимуществ правительству и другим субъектам. Электронное управление увеличивает вовлеченность граждан в процедуры разработки государственной политики, обеспечивая повышение подотчетности (Schuppan, 2009). Оно устраняет барьеры, связанные с материальными и временными затратами граждан на участие в государственных процессах. Эти барьеры снимаются благодаря легкому доступу к информации о государственных услугах и усовершенствованным механизмом взаимодействия с правительством (Sharma et al., 2021). Участвуя в принятии государственных решений посредством систем управления, граждане становятся соавторами решений, непосредственно касающихся их, в сотрудничестве с правительством. Тем самым системы цифрового управления способствуют расширению участия граждан в различных сегментах жизни общества, таких как экономический, социально-культурный и географический.

Кроме того, электронное управление существенно влияет на эффективность и доступность предоставления государственных услуг посредством распространения информации (Sharma et al., 2021). Благодаря цифровизации значительно сокращается время обработки информации, что повышает удовлетворенность пользователей и способствует повышению уровня их участия в жизни страны (Halachmi, 2004). Электронное управление также повышает качество информации, передаваемой партнерам. Исследования показали, что в странах, применяющих онлайн-системы регистрации актов гражданского состояния, сокращается время ожидания и повышается точность ведения записей, что имеет важное значение для эффективного управления (Suthar et al., 2019). Например, внедрение цифровой регистрации рождений и смертей в такой стране, как Гана, привело к заметному увеличению числа регистраций, демонстрируя потенциал электронного управления для улучшения важнейших услуг (Suthar et al., 2019). Внедрение компьютеризированной системы регистрации рождений в Гане привело к увеличению числа регистраций на 15,5 % в период с 2014 по 2017 г.[17] В марте 2023 г. Кения также перешла на электронную регистрацию рождений и смертей[18], что привело к увеличению числа зарегистрированных рождений детей в возрасте до 5 лет до 76 % по сравнению с 65 % в 2014 г.[19]

Эффективность системы электронного управления может оцениваться с различных точек зрения, включая удовлетворенность пользователей, прозрачность, скорость предоставления услуг и уровень соответствия требованиям. Heeks (2003) утверждает, что внедрение электронного управления в развивающихся странах происходит медленно из-за задержек или невыполнения проектов и программ, а также неблагоприятных результатов реализованных проектов. Из-за нехватки экспертных знаний, вызывающей цифровую неграмотность, большинство государств сталкиваются с цифровым разрывом, мешающим успешному электронному

[17] UNICEF. (2018). Assessment of the m-birth project in Ghana. https://clck.ru/3Gf9Jp

[18] Njoya, S. (2023, February 6). Kenya to start issuing digital death and birth certificates. https://clck.ru/3GfFXf

[19] UNICEF. (2023). Country Office Annual Report 2023: Kenya. https://clck.ru/3Gf9MH

управлению (Naqvi et al., 2021). Это подчеркивает, что в большинстве стран глобального Юга внедрение электронного управления ограничено в силу политических, экономических и социально-культурных факторов. Исследования также показывают, что страны, использующие инклюзивные системы мониторинга и оценки, такие как Южно-Африканская Республика во время эпидемии COVID-19 (Naqvi et al., 2021), имеют больше возможностей для оценки эффективности своих процессов электронного управления (Suri & Sushil, 2017). Эти инструменты позволяют правительствам выявлять сектора, в которых наблюдается улучшение, и на основе полученных данных разрабатывать политику, которая способствует предоставлению услуг.

1.4. Проблемы в области электронного управления

Несмотря на многочисленные преимущества инноваций в области электронного управления, рассмотренные выше, у этого процесса есть и недостатки. Одним из них является уязвимость данных, передаваемых по платформам электронного управления. Muttoo и др. (2019) предполагают, что неадекватно разработанные и внедренные процессы электронного управления могут подвергнуть государственные данные и данные граждан угрозам кибербезопасности и незаконному доступу третьих лиц. Это указывает на необходимость интеграции инструментов защиты данных при внедрении технологий электронного управления. Угрозы потери данных и несанкционированного доступа удерживают некоторые страны от перехода с бумажных систем на электронные процессы (Munyoka, 2020). Аналогичным образом граждане опасаются возможного неправомерного использования правительством их информации, хранящейся в электронных системах, без их согласия (Makwanya, 2022). Вероятность неправомерного использования публичной информации неуполномоченными государственными учреждениями очевидна. Несанкционированное распространение личной информации граждан в электронных системах может подорвать их право на неприкосновенность частной жизни[20].

Кроме того, группы населения с недостаточным доступом к Интернету (как из-за отсутствия инфраструктуры, так и из-за низкой покупательной способности) могут оказаться в еще большей изоляции от электронных инноваций в сфере предоставления услуг, что усугубляет цифровой разрыв в обществе (Foster, 2020). Внедрение электронного управления требует наличия электронных инструментов и, что наиболее важно, интернет-грамотности среди пользователей услуг. Отсутствие этих средств и знаний может привести к социальной сегрегации и отчуждению (Palvia & Sharma, 2007). Более того, не все сотрудники государственного сектора, отвечающие за внедрение электронного управления, обладают необходимыми знаниями в области технологий[21]. Следовательно, богатые и технически грамотные граждане и жители районов, где есть подключение к Интернету, возможно, получат доступ к более качественным государственным услугам, чем бедные и неграмотные соотечественники, а также жители районов с плохим или слабым доступом к Интернету. Эта ситуация является заметным недостатком в области цифровизации услуг (Coe et al., 2001)

[20] Zungu, S. (2024). The use of monitoring and evaluation as an improving E-governance for enhanced service delivery: Master thesis. University of Johannesburg.

[21] Там же.

и особенно заметна в Камеруне из-за существенных различий в инфраструктуре между регионами, что ограничивает участие граждан в деятельности правительства посредством электронного управления только лицами, проживающими в городских районах и располагающими ресурсами для приобретения электронных гаджетов и доступа к Интернету.

2. Теоретические основы исследования

Теоретический подход к оценке инноваций в области электронного управления в сфере регистрации актов гражданского состояния в Камеруне основан на двух главных теориях: теории электронного управления и модели принятия технологий (Technological Acceptance Model, TAM). Эти теории обеспечивают прочную основу для понимания того, как технологические инновации могут трансформировать предоставление государственных услуг и способствовать их доступности. Эти теории дают полную возможность оценить электронные новшества, предусмотренные новым законодательством о регистрации актов гражданского состояния.

Теория электронного управления предполагает включение информационно-коммуникационных технологий в процессы государственного управления для совершенствования предоставления услуг, эффективности, прозрачности и доступности (Heeks, 2006). Эта теория подчеркивает преобразующую силу ИКТ в улучшении предоставления государственных услуг и содействии более широкому участию граждан. В отношении нового Закона Камеруна о регистрации актов гражданского состояния теория электронного управления утверждает, что внедрение электронных систем может упростить регистрационные операции, уменьшить бюрократические задержки и повысить точность и согласованность записей актов гражданского состояния. Используя цифровые инструменты, государство может гарантировать гражданам более легкий доступ к средствам регистрации, способствуя инклюзивности и снижая барьеры для участия (Lubis et al., 2024).

Модель принятия технологий служит прочной теоретической основой для понимания того, как пользователи принимают электронные инновации, в частности, для регистрации актов гражданского состояния в Камеруне. Модель предполагает, что основными факторами, влияющими на отношение пользователей к внедрению технологии, являются воспринимаемая полезность и простота использования (Davis et al., 1989). При электронной регистрации актов гражданского состояния воспринимаемая полезность обусловлена эффективностью и доступностью цифровых систем, позволяющих гражданам более оперативно регистрировать такие важные события, как рождение, брак и смерть. Кроме того, важное значение имеет воспринимаемая простота использования: граждане должны считать электронный процесс несложным. Эта модель помогает выявить проблемы при внедрении, такие как низкая технологическая грамотность и инфраструктурные барьеры. Указанные проблемы особенно актуальны в условиях Камеруна, где уровень цифровой грамотности граждан значительно колеблется[22]. Модель применялась в различных

[22] National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

областях, включая электронную коммерцию (Araújo & Casais, 2020), электронное обучение (Al-Gahtani, 2016) и электронное правосудие (Reiling & Contini, 2022). В нашем исследовании мы делаем упор на ожидаемую полезность и воспринимаемую простоту использования электронного управления, чтобы оценить, как эти факторы влияют на отношение пользователей и в конечном итоге на их цель – освоить электронную систему регистрации актов гражданского состояния. Для жителей Камеруна эта задача особенно актуальна, так как правительство страны стремится модернизировать государственные услуги с помощью цифровых технологий.

3. Методы исследования

Настоящее исследование основано на изучении существующей литературы, правовых и политических документов. Такой дизайн позволяет детально изучить новый Закон о регистрации актов гражданского состояния в Камеруне и его новшества в области электронного управления. Качественные исследования необходимы для изучения сложных явлений и понимания условий, в которых они возникают (Creswell & Poth, 2016). Данные для этого исследования были собраны из различных источников, что обеспечивает всестороннюю оценку электронных инноваций и новых законов о регистрации актов гражданского состояния. Эти источники включают: правительственные программные документы, которые важны для понимания позиции правительства и официальной информации, связанной с инновациями в области электронного управления; научные публикации, в которых обсуждаются инновации в области электронного управления и системы регистрации актов гражданского состояния, что дает широкий обзор теоретических основ и эмпирических данных, связанных с темой исследования; а также отчеты неправительственных организаций и международных организаций, которые позволяют внешнюю точку зрения на проблему электронного управления в системах регистрации АГС.

Данные, собранные из этих источников, были проанализированы по тематике. Такой подход предполагает категоризацию, тщательное изучение и выявление шаблонов (тем) в массиве данных. Тематический анализ – это гибкий и ценный инструмент исследования, который позволяет получить разносторонний и подробный обзор данных (Clarke & Braun, 2017). Мы осветим и обсудим основные темы, тенденции и проблемы, связанные с автоматизированными инновациями, предусмотренными новым Законом о регистрации актов гражданского состояния.

Важно признать ограниченность настоящего исследования.

Одним из возможных ограничений методологии данной работы является зависимость от вторичных источников данных, что может привести к искажениям в исходных документах, которые подвергались анализу. Кроме того, отсутствие первичных данных от таких субъектов, как государственные чиновники, население и гражданское общество, сужает рамки анализа. С целью устранить эти методологические недостатки авторы исследования проводили сверку данных официальных правительственных источников, научных публикаций, независимых органов и гражданского общества.

4. Результаты исследования: обзор электронных инноваций в новом законодательстве Камеруна

Анализ текста Закона № 2024/016 от 23 декабря 2024 г. о создании системы регистрации актов гражданского состояния, в частности его положений, касающихся электронного управления регистрацией актов гражданского состояния, позволил выявить следующие нововведения.

4.1. Технологические инновации

Закон 2024 г. вводит несколько важных определений и правовых основ, необходимых для понимания использования электронного управления при регистрации актов гражданского состояния в Камеруне. Согласно новому закону, электронное удостоверение – это электронный документ, защищенный электронной подписью его пользователя, который после проверки подтверждает подлинность его содержимого. Утвержденный центр сертификации выдает квалифицированное электронное удостоверение. Эти определения закладывают основу для защищенной и аутентичной электронной записи и архивирования жизненно важных событий. Нововведения гарантируют подлинность документов о гражданском состоянии, что важно для сохранения целостности записей. Кроме того, они обеспечивают дополнительную степень безопасности и надежности, гарантируя, что население может доверять документам, предоставляемым в электронном виде.

Кроме того, в ст. 83 Закона от 2024 г. вводится уникальный личный идентификационный номер (Unique Personal Identification Number, UPIN), присваиваемый при рождении, что упрощает процессы идентификации в рамках систем гражданского состояния Камеруна. Предполагается, что этот уникальный идентификатор упростит коммуникации между гражданами и государственными учреждениями, сократив количество двойных идентификаций и бюрократических проволочек. Кроме того, закон предусматривает цифровую запись и архивирование свидетельств, связанных с жизненно важными событиями, что значительно улучшает возможности управления данными и позволяет более эффективно извлекать данные при необходимости.

4.2. Совершенствование предоставления услуг

Одним из ключевых примечательных аспектов нового закона является положение об электронном декларировании жизненно важных событий, таких как рождение, заключение брака и смерть (разд. 9). Переход от чисто традиционных бумажных процедур к компьютеризированным системам повышает доступность для граждан, ускоряет процесс регистрации и снижает административную нагрузку на граждан и государственных служащих. Кроме того, Закон 2024 г. вводит автоматизацию декларирования жизненно важных событий, а также составления, выдачи и архивирования документов о гражданском состоянии и сбора статистики (разд. 80). Такая автоматизация повышает эффективность и точность процессов регистрации актов гражданского состояния. Однако порядок подачи электронных деклараций будет определен в последующих нормативных актах, что, возможно, позволит адаптировать этот процесс к потребностям пользователей. Ранее утрата оригинала документа о гражданском состоянии требовала длительного судебного разбирательства для получения нового, однако новый закон позволяет в случае утери получать копии

документов о гражданском состоянии из Национальной базы данных актов гражданского состояния (разд. 62(3)).

Кроме того, закон расширяет способы публикации уведомлений о вступлении в брак, начиная с распечатки и заканчивая размещением в Интернете на вебсайте местного совета, и вводит электронную публикацию уведомлений о намерении вступить в брак (разд. 17). Это нововведение укрепляет связи между службами регистрации актов гражданского состояния, повышает прозрачность и ускоряет процедуру регистрации брака. Примечательно, что документы о гражданском состоянии в Камеруне теперь можно подавать в печатном и цифровом виде, причем оба формата имеют одинаковую юридическую силу (разд. 29). Такой двойной подход гарантирует гражданам гибкость в получении документов, тем самым улучшая общее качество обслуживания. Кроме того, в разд. 126 закона указано, что полное внедрение электронного управления при регистрации на государственной службе в Камеруне начнется с пилотного этапа. В частности, это положение закона придает юридическую силу «актам гражданского состояния, составленным в рамках экспериментальных работ по компьютеризации записей актов гражданского состояния…» Раздел 70(2) Закона 2024 г. предусматривает переход к цифровому администрированию, указывая, что любой центр записи актов гражданского состояния, полностью перешедший на цифровую форму, будет освобожден от ведения реестров на бумажных носителях. Это свидетельствует о приверженности правительства постепенному преобразованию системы регистрации актов гражданского состояния в Камеруне с помощью электронного управления.

4.3. Управляемость и подотчетность

Создание Национальной базы данных актов гражданского состояния – это главная особенность нового закона, который предусматривает централизованное хранение всех документов о гражданском состоянии в Камеруне (разд. 30). В базе данных будут храниться «вся информация, данные, документы, копии и формы как в бумажном, так и в цифровом виде, связанные с декларированием жизненно важных событий и составлением документов о гражданском состоянии» (разд. 77). Перечисленные данные хранятся и обрабатываются либо в печатном, либо в электронном виде органом по управлению гражданским состоянием (разд. 78(3)). Создание этой базы данных будет способствовать целостности данных и повысит их доступность как для граждан, так и для должностных лиц, занимающихся проблемами гражданского состояния. Ожидается, что объединение записей актов гражданского состояния в одном месте повысит эффективность управления, сохраняя при этом актуальность и точность данных.

Закон также вводит электронные возражения против заключения брака, позволяя частным лицам подавать свои протесты с помощью цифровых каналов (разд. 42). Тот же компьютеризированный канал применяется для запросов о выдаче разрешения на публикацию объявлений о расторжении брака, направляемого компетентному государственному юристу (разд. 18). Это рационализирует процедуру, делая ее более эффективной и экономя время граждан и судебных органов.

4.4. Защита данных и нормативная правовая база

Закон подчеркивает важность защиты и безопасности данных. В разд. 82 говорится, что «личные данные о гражданском состоянии, содержащиеся в национальной базе данных о гражданском состоянии, должны быть защищены в соответствии с законами о защите персональных данных». Это положение перекликается с Законом Камеруна № 2024/017 от 23 декабря 2024 г. о защите персональных данных. Это нововведение отражает стремление правительства сохранить частную жизнь и безопасность граждан в условиях развития цифровых технологий. Кроме того, разд. 82 предоставляет регистраторам АГС и их секретарям прямой доступ к данным о гражданском состоянии, относящимся к их центрам. Такой же доступ предоставляется государственным органам, подключенным к национальным системам регистрации актов гражданского состояния, для проведения специальных или общих консультаций. Для обеспечения эффективности и безопасности закон гарантирует, что технические характеристики и процедура электронной передачи данных о гражданском статусе должны соответствовать закону, регулирующему электронные коммуникации в Камеруне (разд. 83). Электронные коммуникации в Камеруне регулируются Законом № 2010/013 от 21 декабря 2010 г. с поправками и дополнениями, внесенными Законом № 2015/016 от 20 апреля 2015 г.

Закон 2024 г. предусматривает, что большинство аспектов внедряемых цифровых инноваций будут регулироваться отдельными правовыми документами и нормативными актами. К ним относятся: порядок выдачи документов о гражданском состоянии в электронном виде (разд. 29(5)); порядок получения подписей на электронных свидетельствах о браке (разд. 41(2)); порядок доступа к материалам Национальной базы данных о гражданском состоянии, а также выдачи и заверения документов о гражданском состоянии (разд. 79); порядок автоматизированной обработки документов о гражданском состоянии (разд. 80); особенности и порядок использования и присвоения уникального личного идентификационного номера (разд. 81(3)); а также перечень административных органов и порядок доступа к данным в Национальной базе данных о гражданском состоянии (разд. 82(4)). Предполагаемая нормативно-правовая база, вероятно, должна гарантировать соответствие всех электронных коммуникаций правовым стандартам, снижая риск мошенничества и обеспечивая безопасность персональных данных. Кроме того, благодаря выбору отдельных надежных правовых рамок, регулирующих функциональные возможности новой модели электронного управления и защиту прав личности, закон создает безопасную и структурированную среду для регистрации актов гражданского состояния. Такой акцент на инструментах управления имеет решающее значение для установления общественного доверия к системе, поскольку граждане будут иметь четкое представление о том, как хранятся их данные и осуществляется доступ к ним.

4.5. Технологическая инфраструктура в Камеруне

Камерун добился значительных успехов в секторе ИКТ, в частности, благодаря принятию Национального стратегического плана в области ИКТ до 2020 г., в котором цифровая экономика рассматривается как ключевой фактор развития[23]. Национальная

[23] Toussi, S. (2019, September 12). Overview of Cameroon's Digital Landscape. CIPESA. https://clck.ru/3Gf9m2

волоконно-оптическая магистраль протяженностью около 12 тысяч километров соединила 209 из 360 регионов страны. Министерство почты и телекоммуникаций Камеруна сообщило, что к 2018 г. 83 % граждан пользовались услугами мобильной связи, а уровень проникновения Интернета составил 35 %[24]. Согласно Индексу развития ИКТ за 2024 г., Камерун в настоящее время занимает 31-е место из 47 стран с результатом 44,2 балла[25].

Национальный стратегический план в области ИКТ за 2020 г. охватывает восемь ключевых областей, что соответствует перспективам развития страны до 2035 г. Для стимулирования развития цифровых государственных услуг в Камеруне было создано несколько государственных учреждений[26]. На основе этой институциональной структуры был предпринят ряд инициатив в области электронного управления. Среди них цифровизация работы государственных служащих, государственных финансов, ведения списков избирателей, таможенных операций и транспортных документов и управления этими сферами[27]. Другие инновации в области электронного управления реализуются путем введения электронных налогов, электронных виз и электронной коммерции[28]. В рамках Стратегического плана по восстановлению системы регистрации актов гражданского состояния в Камеруне (2018–2022 гг.) в 2018 г. разработан план цифровизации системы регистрации АГС в качестве основы для Закона о системах регистрации актов гражданского состояния от 2024 г. Согласно плану, целью является повышение эффективности предоставления услуг через создание платформы, объединяющей систему регистрации актов гражданского состояния и другие секторы, такие как институт идентификации личности Министерства юстиции, транспорта и здравоохранения.

5. Обсуждение

Цель настоящей статьи состоит в изучении электронных инноваций, введенных в систему регистрации актов гражданского состояния Камеруна в соответствии с новым Законом от 23 декабря 2024 г., а также их последствий для сферы услуг, управления и вовлеченности граждан. Используя качественный подход, авторы проанализировали существующую литературу, политические и юридические документы, чтобы оценить эффективность новой системы электронного управления в секторе регистрации актов гражданского состояния. Был проведен тематический анализ, классифицированы основные темы и проблемы, связанные с новым законом. Исследование выявило ряд важных инноваций, введенных Законом 2024 года, включая концепции цифровых удостоверений и квалифицированных электронных удостоверений, введение уникального личного идентификационного номера,

24 Ministry of Posts and Telecommunication (2018). Posts, Telecommunications, and ICT: Precious assets of the seven-year mandate. https://clck.ru/3Gf9pe

25 Ecofin agency. (2024, July 16). ICT Development Index 2024: Ranking of African Countries. https://clck.ru/3Gf9tk

26 Telecommunications Regulatory Board (ART); the National Agency for ICT (ANTIC); and the National Centre for the Development of Computer Services (CENADI).

27 Alypova, S. (2024). E-government Development in Cameroon. Centre for African Studies, HSE University. https://clck.ru/3Gf9zu

28 Там же.

электронного декларирования жизненно важных событий, внедрение электронных подписей и создание Национальной базы данных о гражданском состоянии. Другими важными новшествами являются автоматизация регистрации АГС и публикация брачных свидетельств онлайн. Эти нововведения приводят систему регистрации актов гражданского состояния Камеруна в соответствие с моделью критического потока в электронном управлении. Кроме того, инновации соответствуют категориям взаимодействия «правительство с правительством» (G2G) и «правительство с гражданами» (G2C).

Основные выводы исследования демонстрируют наличие в новом законе существенных нововведений, но выявляют проблемы с его внедрением, связанные с уровнем технологической грамотности, технологической инфраструктуры и доступностью Интернета в Камеруне. Эти проблемы влияют на предоставление услуг и подотчетность в сфере управления. Что касается электронного правительства, то в соответствующем рейтинге Организации Объединенных Наций за 2024 г. Камерун занимает 155-е место из 193 стран (139-е место в 2004 г.) и 105-е место по уровню электронного участия граждан (84-е место в 2004 г.)[29]. При охвате Интернетом менее 50 %, согласно индексу сетевой готовности страны, в 2024 г. страна находится на 113-м месте из 133 стран с зафиксированным улучшением в сфере управления[30]. Хотя спрос на интернет-услуги постоянно растет, в некоторых сельских районах они практически недоступны.

Одним из важнейших результатов стало создание Национальной базы данных актов гражданского состояния для централизации и хранения документов о гражданском состоянии. Это нововведение имеет огромное значение, поскольку Национальная база данных обладает потенциалом для повышения целостности данных, культуры хранения записей и модернизации доступа к ценной информации. Это очень важно для преобразования разрозненной системы регистрации актов гражданского состояния во взаимосвязанную, эффективную систему, которая эффективно удовлетворяет потребности граждан. Автоматизация операций по регистрации актов гражданского состояния станет еще более эффективной за счет уменьшения бюрократических задержек и ошибок. Кроме того, внедрение электронного декларирования жизненно важных событий – рождений, браков и смертей – отражает значительное изменение парадигмы взаимодействия между гражданами и государственными службами. Это нововведение сокращает время обработки и повышает доступность данных, особенно для маргинализированных слоев населения, которые могут столкнуться с трудностями при традиционном декларировании[31]. Указанные преобразования находят отклик в обществе; это означает, что граждане осваивают технологии, основываясь на воспринимаемой простоте их использования и полезности (Reiling & Contini, 2022).

Внедрение электронных удостоверений является важной вехой на пути к обеспечению подлинности и безопасности документов о гражданском состоянии. Закон 2024 г., предусматривающий использование цифровых подписей и алгоритмов кодирования, направлен на повышение целостности и достоверности документов о гражданском состоянии в Камеруне. Это нововведение соответствует принципам

29 UN E-Government Knowledgebase. https://clck.ru/3GfA9A

30 Portulans Institute. (2024). Network Readiness Index 2024: Cameroon. https://clck.ru/3GfABt

31 Zewoldi, Y. (2019). Snapshot of Civil Registration and Vital Statistics in Cameroon. Centre of Excellence for Civil Registration and Vital Statistics. https://clck.ru/3GfADM

теории электронного управления, которая отмечает преобразующие возможности ИКТ в улучшении предоставления государственных услуг (Heeks, 2006). Кроме того, введение уникального личного идентификационного номера упрощает архивирование записей актов гражданского состояния, управление ими и поиск информации. Номер служит уникальным идентификатором для граждан, упрощая процедуру регистрации и сводя дублирование к минимуму.

Полученные результаты согласуются с предыдущими исследованиями преимуществ электронного управления в сфере регистрации актов гражданского состояния и в других областях. Например, исследования, проведенные в таких странах, как Эстония и Кения, показали, что централизованные компьютеризированные системы могут значительно улучшить предоставление услуг, повысить уровень удовлетворенности граждан и снизить бюрократическую нагрузку (Tammpuu & Masso, 2018). Кроме того, модель регистрации рождений в Гане доказывает, что цифровизация в этой области значительно увеличивает количество заявлений о жизненно важных событиях[32]. Аналогичным образом, внедряя электронное управление в процессы регистрации актов гражданского состояния, законодательная власть Камеруна стремится повысить эффективность и доступность услуг для граждан и других учреждений с помощью централизованных записей, цифровых сертификатов и уникального личного идентификационного номера. Камерун может извлечь важные уроки из успехов этих стран, гарантируя эффективную реализацию своих инноваций с помощью специально разработанной нормативно-правовой базы. Однако, хотя ученые подчеркивают достоинства электронного управления, они также отмечают необходимость устранить инфраструктурные барьеры и возможное общественное противодействие инновациям[33].

Результаты исследования перекликаются с теорией электронного управления. Эта теория предполагает, что внедрение ИКТ в процессы государственного управления может повысить прозрачность, подотчетность и участие граждан (Heeks, 2006). Наши результаты подтверждают эту теорию, поскольку внедрение уникального личного идентификационного номера, электронных деклараций о жизненно важных событиях, возражений против бракосочетания, электронных подписей для оформления брака и электронной публикации брачных заявлений о расторжении брака соответствуют принципам доступности и прозрачности. Кроме того, полученные результаты относятся к модели принятия технологий. Данная модель утверждает, что явная простота использования и предполагаемая полезность в значительной степени определяют принятие технологии гражданами (Davis et al., 1989). Новый закон направлен на повышение удобства использования операций по регистрации актов гражданского состояния путем автоматизации транзакций и внедрения электронных деклараций, подписей и сертификатов. Эффективное применение цифровых инноваций в системе регистрации актов гражданского состояния в Камеруне в значительной степени зависит как от функциональности системы, так и от того, насколько легко сотрудники службы записи актов гражданского состояния и граждане могут получить доступ к новым технологиям и использовать их. Таким образом, если граждане сочтут автоматизированную систему актуальной и простой в использовании, они, скорее всего, положительно воспримут нововведения.

---

32 UNICEF. (2018). Assessment of the m-birth project in Ghana. https://clck.ru/3GfAKK

33 Zungu, S. (2024). The use of monitoring and evaluation as an improving E-governance for enhanced service delivery. Master thesis. University of Johannesburg.

Несмотря на важные выводы о потенциале Закона 2024 г. для повышения эффективности и доступности системы регистрации актов гражданского состояния, следует признать возможность альтернативного анализа. Например, успех новой компьютеризированной системы регистрации актов гражданского состояния может зависеть от способности и желания правительства усовершенствовать технологическое оснащение и организовать регулярное обучение регистраторов актов гражданского состояния, секретарей и других заинтересованных сторон, вовлеченных в этот процесс. Если эти основополагающие факторы не будут должным образом учтены, прогнозируемые результаты могут оказаться не такими, как ожидалось. Более того, успех нового закона может зависеть от механизмов регулирования, политической воли и способности правительственных учреждений обеспечить соблюдение нового закона. Кроме того, серьезную угрозу представляет существующий в Камеруне цифровой разрыв, особенно между городскими и сельскими районами. Если не устранить неравенство в доступе к технологиям, цифровые инновации могут непреднамеренно усугубить существующее социальное неравенство.

Исследование имеет ряд ограничений. Во-первых, зависимость от вторичных данных может привести к необъективности, поскольку в новом законе не учитывается мнение основных участников процесса внедрения инновационной цифровой системы. Кроме того, авторы исследовали недавно принятое законодательство, эффективное применение которого требует принятия дополнительных нормативных актов. Эмпирических данных о удовлетворенности пользователей и эффективности цифровой системы недостаточно, поскольку до сих пор никаких исследований по этому вопросу не проводилось. Это ограничивает возможность сделать вывод о практических успехах внедряемых цифровых инноваций.

Дальнейшие исследования могли бы включать оценку долгосрочных последствий цифровых инноваций для системы регистрации актов гражданского состояния в Камеруне. Полезны были бы также эмпирические работы по сбору качественных первичных данных от основных участников и пользователей системы регистрации актов гражданского состояния, что позволило бы получить глубокое представление об опыте граждан и областях, требующих улучшения. Кроме того, важны исследования взаимосвязи ИКТ и социальной интеграции. Это поможет выявить способы гарантировать, что все граждане имеют доступ к этим инновациям и извлекают выгоду из них без какой-либо дискриминации.

6. Рекомендации

Чтобы усилить правоприменение и повысить эффективность цифровых инноваций, предусмотренных новым Законом о регистрации актов гражданского состояния в Камеруне, следует рассмотреть ряд мер. Результаты исследования указывают на необходимость повысить уровень развития технологической инфраструктуры в стране для обеспечения успеха инноваций в области электронного управления. Правительству следует шире использовать преимущества развития и расширения возможностей подключения к Интернету, особенно в сельских и малообеспеченных поселениях. Это включает предоставление комплектов ИКТ оборудования и других ресурсов центрам регистрации актов гражданского состояния для облегчения эффективного сбора данных, управления ими и передачи в централизованное хранилище. Как подчеркивает Национальный институт статистики, это гарантирует гражданам

доступ к компьютеризированным службам регистрации актов гражданского состояния и сократит цифровой разрыв[34].

Кроме того, эффективное применение цифровых технологий в соответствии с новым законом требует, чтобы государственные служащие и сотрудники службы записи актов гражданского состояния были хорошо обучены использованию цифровых инструментов. Следует разработать инклюзивные учебные программы для повышения их технических навыков и ознакомления с новыми процессами. Такие программы повышения квалификации должны быть постоянными, чтобы сотрудники были в курсе технического прогресса и лучших практик в данной области. Это минимизирует сопротивление преобразованиям и обеспечит легкое освоение новых систем[35]. Кроме того, регулярный мониторинг и оценка правоприменительной практики необходимы для выявления трудностей и внесения соответствующих корректив. Правительству следует создать механизм мониторинга для отслеживания эволюции нового закона и оценки его влияния на службы регистрации актов гражданского состояния. Для совершенствования работы системы необходимо обеспечить постоянную обратную связь с заинтересованными сторонами.

Новый закон содержит также некоторые положения, требующие принятия дополнительных нормативных актов и руководящих принципов для обеспечения соблюдения этого закона. Правительству следует ускорить разработку этих нормативных актов, чтобы обеспечить, среди прочего, четкие условия, касающиеся процедур электронного декларирования, выдачи электронных удостоверений, формирования и выдачи уникального личного идентификационного номера и функционирования Национальной базы данных. Это гарантирует надежность и соответствие требованиям во всех центрах регистрации актов гражданского состояния (Heeks, 2006). Безопасность личных данных о гражданском состоянии важна для обеспечения общественного доверия к инновационной системе. Правительству следует внедрить в работу Национальной базы данных надежные стратегии защиты данных, включая шифрование, ограничения доступа и регулярные проверки, чтобы обеспечить безопасность чувствительной информации. Кроме того, необходимо строго гарантировать соответствие Закону о защите персональных данных. С помощью этих механизмов правительство обеспечит прозрачность и подотчетность в процессе правоприменения и продемонстрирует готовность решать любые проблемы, связанные с безопасностью и конфиденциальностью данных. Достижение этих целей укрепит общественное доверие к системе, гарантируя ее успех и снижая сопротивление.

Кроме того, среди основных стратегий успешного внедрения инноваций в области электронного управления, предусмотренных новым Законом о регистрации актов гражданского состояния, нужно выделить привлечение заинтересованных сторон и просвещение населения. Ключевыми участниками являются государственные учреждения, служащие, гражданское общество и общественные лидеры. Они должны быть в полной мере вовлечены в разработку нормативных актов, политики в области обучения и механизмов мониторинга. Их участие и обратная связь

---

34 National Institute of Statistics. (2023). Rapport sur les statistiques de l'état civil au Cameroun (2018–2022). https://clck.ru/3Gf8Uq

35 Zewoldi, Y. (2019). Snapshot of Civil Registration and Vital Statistics in Cameroon. Centre of Excellence for Civil Registration and Vital Statistics. https://clck.ru/3GfADM

могут дать ценные перспективы и помочь в устранении возможных недостатков. Опять же, для информирования граждан об инновациях электронного управления в сфере регистрации актов гражданского состояния и их преимуществах необходимы образовательные и разъяснительные мероприятия. Для охвата широкой аудитории в этих кампаниях должны использоваться различные средства коммуникации, включая радио, телевидение, социальные сети, плакаты, местные собрания, церкви и другие общественные мероприятия. Население должно получать четкую и доступную информацию о важности регистрации актов гражданского состояния, соответствующих правах и о том, как пользоваться компьютеризированной системой. Наряду с информационно-просветительскими кампаниями правительству следует принять программы, направленные на повышение цифровой грамотности, главным образом в сельских районах и районах с недостаточным уровнем жизни, чтобы дать гражданам возможность эффективного доступа к цифровым системам.

Заключение

В работе были рассмотрены цифровые инновации, закрепленные в Законе 2024 г., регулирующем систему регистрации актов гражданского состояния в Камеруне. Исследование дает ценную информацию о том, как эти инновации могут изменить процессы регистрации АГС. Внедрение электронного декларирования гражданского состояния, цифровых удостоверений, уникального персонального идентификационного номера и создание Национальной базы данных актов гражданского состояния являются важными нововведениями, которые повышают эффективность, удобство для пользователей и надежность процессов в этой области. Эти результаты особенно примечательны тем, что они подчеркивают потенциал ИКТ в преобразовании государственного управления и повышении качества предоставляемых услуг. Одним из главных и неожиданных результатов этого исследования является то, что некоторые ключевые аспекты компьютеризированных инноваций могут быть реализованы только с помощью методов и процедур, определенных нормативными актами. Эти нормативные акты еще не приняты, и существует вероятность, что в ближайшее время они не будут приняты, что может подорвать полноценное внедрение цифровых инноваций.

Результаты исследования имеют важное значение для системы регистрации актов гражданского состояния и управления государственным сектором в Камеруне. Через внедрение цифровых технологий новый закон модернизирует процедуры регистрации актов гражданского состояния, сокращает бюрократические проволочки и повышает точность и достоверность записей. Это может повысить эффективность предоставления государственных услуг, что принесет пользу гражданам и государственным учреждениям. Исследование вносит свой вклад в научный дискурс, представляя содержательную оценку цифровых инноваций, заложенных в новом Законе о регистрации АГС в Камеруне. Существуют научные работы, посвященные применению электронного управления при регистрации актов гражданского состояния в таких странах, как Кения, Гана, Южная Африка и Эстония, однако до сих пор не было проведено исследований, посвященных ситуации в Камеруне. Настоящая статья восполняет этот пробел. В работе проведена оценка проблем и возможностей электронного управления, предусмотренных новым законом, и его потенциальное влияние на операции по регистрации актов гражданского состояния. Полученные результаты

подчеркивают необходимость дальнейшего изучения долгосрочных аспектов инноваций в области электронного управления и факторов, влияющих на их успех.

Результаты исследования имеют решающее значение для развития системы регистрации актов гражданского состояния и управления государственным сектором в Камеруне. Нововведения могут модернизировать процессы регистрации актов гражданского состояния в Камеруне, сделав их более взаимосвязанными, эффективными, доступными и надежными. Изложенные рекомендации по вовлечению заинтересованных сторон и повышению осведомленности общественности демонстрируют разработчикам государственной политики и практикам необходимость сотрудничества при внедрении цифровой системы. Это гарантирует, что граждане получат знания и навыки доступа к цифровым услугам. В исследовании также подчеркивается важность обеспечения безопасности и конфиденциальности данных при внедрении электронного управления. Обеспечивая защиту личных данных о гражданском состоянии, новый закон направлен на укрепление общественного доверия к новой системе. Это имеет решающее значение для успешного внедрения услуг цифровой регистрации актов гражданского состояния и общей эффективности инициатив в области электронного управления.

Список литературы

Albert, I. O. (2009). Whose E-Governance?: A Critique of Online Citizen Engagement In Africa. *International Journal of eBusiness and eGovernment Studies*, *1*(1), 27–40.

Al-Gahtani, S. S. (2016). Empirical investigation of e-learning acceptance and assimilation: A structural equation model. *Applied Computing and Informatics*, *12*(1), 27–50.

Araújo, T., & Casais, B. (2020). Customer acceptance of shopping-assistant chatbots. In *Marketing and Smart Technologies: Proceedings of ICMarkTech 2019* (pp. 278–287). Singapore: Springer.

Bannister, F., & Connolly, R. (2012). Defining e-Governance. *e-Service Journal*, *8*(2), 3–25. https://doi.org/10.2979/eservicej.8.2.3

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Coe, A., Paquet, G., & Roy, J. (2001). E-governance and smart communities: a social learning challenge. *Social Science Computer Review*, *19*(1), 80–93.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). Technology acceptance model. *Journal of Management Science*, *35*(8), 982–1003.

Djossa-Tchokoté, I., Teutio, A. O. N., & Nyongo, A. S. A. (2024). E-Governance, Digitized Tax Procedures and SME's Business Process Performance in Cameroon. *iBusiness*, *16*(3), 65–84. https://doi.org/10.4236/ib.2024.163006

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International Journal of the Computer, the Internet and Management*, *10*(2), 1–22.

Foster, K. (2020). Smarten Up: Paths to bottom-up smart cities and the risks of top-down smart governance. *Smart Cities Paper Series: Smart Governance in South African Cities*.

Grigalashvili, V. (2022). E-government and E-governance: Various or Multifarious Concepts. *International Journal of Scientific and Management Research*. *5*(01).183–196. https://doi.org/10.37502/ijsmr.2022.5111

Halachmi, A. (2004). E-government theory and practice: The evidence from Tennessee (USA). In M. Holzer, M. Zhang, & K. Dong (Eds.), *Frontiers of Public Administration: Proceedings of the Second Sino-U.S. International Conference: Public Administration in the Changing World* (pp. 24–43). United Nations Public Administration Network.

Heeks, R. (2003). E-Government in Africa: Promise and practice. *Information Polity*, *7*(23), 97–114. https://doi.org/10.3233/ip-2002-0008

Heeks, R. (2006). *Implementation and managing e-Governance*. London: Sage publications Ltd.

Kaisara, G., & Pather, S. (2011). The e-Government evaluation challenge: A South African Batho Pele-aligned service quality approach. *Government Information Quarterly*, *28*(2), 211–221. https://doi.org/10.1016/j.giq.2010.07.008

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In M. E. Compton, & P. Hart (Eds.), *Great Policy Successes* (pp. 143–160). Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008

Lubis, S., Purnomo, E. P., Lado, J. A., & Hung, C. F. (2024). Electronic governance in advancing sustainable development goals through systematic literature review. *Discover Global Society*, *2*(1) 77. https://doi.org/10.1007/s44282-024-00102-3

Makwanya, M. (2022). Digital practice for social work in Zimbabwe: Success, challenges and opportunities. In A. L. Peláez, S. Suh, & S. Zelenev (Eds.), *Digital Transformation and Social Well-Being* (pp. 160–168). Routledge.

Munyoka, W. (2020). Electronic government adoption in voluntary environments–a case study of Zimbabwe. *Information Development*, *36*(3), 414–437. https://doi.org/10.1177/0266666919864713

Muttoo, S. K., Gupta, R., Pal, S. K., & Muttoo, S. K. (2019). *E-Governance in India* (pp. 13–25). Singapore: Springer. https://doi.org/10.1007/978-981-13-8852-1

Naqvi, S. A. M., Alyas, T., Tabassum, N., Namoun, A., & Naqvi, H. H. (2021). Post Pandemic World and Challenges for E-Governance Framework. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2630–2636. https://doi.org/10.30534/ijatcse/2021/1571032021

Oliveira, T. A., Oliver, M., & Ramalhinho, H. (2020). Challenges for Connecting Citizens and Smart Cities: ICT, e-Governance and Blockchain. *Sustainability*, *12*(7), 2926. https://doi.org/10.3390/su12072926

Palvia, S. C. J., & Sharma, S. S. (2007). E-government and e-governance: definitions/domain framework and status around the world. In *International Conference on E-governance* (Vol. 5, No. 1, pp. 1–12).

Prashar, K., & Bawa, S. S. (2023). Studying the Effect of Artificial Intelligence on E-Governance. In P. Tyagi, S. Grima, K. Sood, B. Balamurugan, E. Özen, & T. Eleftherios (Eds.), *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy (Contemporary Studies in Economic and Financial Analysis, Vol. 110A)* (pp. 87–101). Emerald Publishing Limited, Leeds. https://doi.org/10.1108/S1569-37592023000110A005

Reiling, D., & Contini, F. (2022). E-Justice Platforms: Challenges for Judicial Governance. *International Journal for Court Administration*, *13*(1), 6. https://doi.org/10.36745/ijca.445

Schuppan, T. (2009). E-Government in developing countries: Experiences from sub-Saharan Africa. *Government Information Quarterly*, *26*(1), 118–127. https://doi.org/10.1016/j.giq.2008.01.006

Sevidzem, M. C. (2024). Use of ICT and the Application of E-Governance Strategies in Service Delivery by Local Councils in Cameroon: The Case of Local Councils in the Bamenda Municipality. *PanAfrican Journal of Governance and Development (PJGD)*, *5*(1), 3–27. https://doi.org/10.46404/panjogov.v5i1.5354

Sharma, S., Kumar Kar, A., & Gupta, M. P. (2021). Unpacking Digital Accountability: Ensuring efficient and answerable e-governance service delivery. In *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance* (pp. 260–269). https://doi.org/10.1145/3494193.3494229

Suri, P. K., & Sushil. (Eds.) (2017). *Strategic Planning and Implementation of E-Governance*, Springer.

Suthar, A. B., Khalifa, A., Yin, S., Wenz, K., Ma Fat, D., Mills, S. L., ... & Mrkic, S. (2019). Evaluation of approaches to strengthen civil registration and vital statistics systems: a systematic review and synthesis of policies in 25 countries. *PLoS Medicine*, *16*(9), e1002929. https://doi.org/10.1371/journal.pmed.1002929

Tammpuu, P., & Masso, A. (2018). 'Welcome to the virtual state': Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies*, *21*(5), 543–560. https://doi.org/10.1177/1367549417751148

Umbach, G., & Tkalec, I. (2022). Evaluating e-governance through e-government: Practices and challenges of assessing the digitalisation of public governmental services. *Evaluation and program planning*, *93*, 102–118. https://doi.org/10.1016/j.evalprogplan.2022.102118

Xin, G., Esembe, E. E., & Chen, J. (2023). The mixed effects of e-participation on the dynamic of trust in government: Evidence from Cameroon. *Australian Journal of Public Administration*, *82*(1), 69–95. https://doi.org/10.1111/1467-8500.12569

Сведения об авторах

Ндиюн Роберт Кошо – PhD в области политологии, пост-док, кафедра по связям с общественностью, Технологический университет Тшване
Адрес: Южно-Африканская Республика, 0183, г. Претория, ул. Штаатсартиллери, парк Филипа Нела
ORCID ID: https://orcid.org/0000-0002-6435-0494
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57762430700
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JCD-5501-2023
Google Scholar ID: https://scholar.google.com/citations?user=siNlKWQAAAAJ

Муконза Рикки Муньярадзи – доктор технологии в области государственного управления, доцент в области государственного управления, кафедра по связям с общественностью, Технологический университет Тшване
Адрес: Южно-Африканская Республика, 0183, г. Претория, ул. Штаатсартиллери, парк Филипа Нела
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.07.45 / Право и научно-технический прогресс
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 18 января 2025 г.
Дата одобрения после рецензирования – 31 января 2025 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:347.6:004.9:004.056
EDN: https://elibrary.ru/eaqyqj
DOI: https://doi.org/10.21202/jdtl.2025.1

Digital Transformation of Civil Registration System in Cameroon: Innovations in e-Governance

Robert Kosho Ndiyun ✉
Tshwane University of Technology, Pretoria, South Africa

Ricky Munyaradzi Mukonza
Tshwane University of Technology, Pretoria, South Africa

Keywords

Cameroon,
civil status act,
data protection,
digital literacy,
digital technologies,
e-governance,
e-government,
law,
legislation,
public service

Abstract

Objective: to study the innovative transformations in the field of e-Governance introduced into Cameroon's civil registration system during the 2024 legislative reforms. The focus is on assessing the impact of these transformations on improving governance efficiency, transparency, accessibility of services for citizens, as well as improving statistical accounting of vital events.

Methods: the work uses general scientific methods of analysis and synthesis, classification, systematic and functional approaches, as well as formal legal and comparative legal methods.

Results: the research shows that measures like introduction of electronic declaration of civil status acts, creation of a national database and transition to electronic certificates can dramatically improve the efficiency and accessibility of services for the population. However, the authors emphasize that the successful implementation of digital innovations requires overcoming significant barriers, such as insufficient technological equipment, limited Internet access, and low digital literacy of citizens. These challenges make it necessary to develop additional regulatory and support mechanisms. Particularly important is the balance between digitalization and ensuring the rights of citizens in the context of electronic registration.

✉ Corresponding author

Scientific novelty: the work provides unique empirical data on digitalization of public services in Cameroon. This is especially important for the countries of the global South, where such transformations are slow and fragmentary. The study makes a significant contribution to the scientific debate by expanding understanding of digital technology adoption models through the lens of expected usefulness and perceived ease of use in developing countries.

Practical significance: recommendations for legislators, government officials and other stakeholders were developed. The authors emphasize the need to adopt a regulatory framework as soon as possible, introduce educational programs for employees and citizens, and ensure access to digital technologies. These measures aim at creating a sustainable infrastructure for an effective transition to electronic systems and improving the quality of public services. The work contributes to the study of public governance digitalization, offering both theoretical concepts and practical solutions that can be adapted for other countries with similar challenges.

For citation

Ndiyun, R. K., & Mukonza, R. M. (2025). Digital Transformation of Civil Registration System in Cameroon: Innovations in e-Governance. *Journal of Digital Technologies and Law, 3*(1), 7–34. https://doi.org/10.21202/jdtl.2025.1

References

Albert, I. O. (2009). Whose E-Governance?: A Critique of Online Citizen Engagement In Africa. *International Journal of eBusiness and eGovernment Studies*, *1*(1), 27–40.

Al-Gahtani, S. S. (2016). Empirical investigation of e-learning acceptance and assimilation: A structural equation model. *Applied Computing and Informatics*, *12*(1), 27–50.

Araújo, T., & Casais, B. (2020). Customer acceptance of shopping-assistant chatbots. In *Marketing and Smart Technologies: Proceedings of ICMarkTech 2019* (pp. 278–287). Singapore: Springer.

Bannister, F., & Connolly, R. (2012). Defining e-Governance. *e-Service Journal*, *8*(2), 3–25. https://doi.org/10.2979/eservicej.8.2.3

Clarke, V., & Braun, V. (2017). Thematic analysis. *The Journal of Positive Psychology*, *12*(3), 297–298. https://doi.org/10.1080/17439760.2016.1262613

Coe, A., Paquet, G., & Roy, J. (2001). E-governance and smart communities: a social learning challenge. *Social Science Computer Review*, *19*(1), 80–93.

Creswell, J. W., & Poth, C. N. (2016). *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). Technology acceptance model. *Journal of Management Science*, *35*(8), 982–1003.

Djossa-Tchokoté, I., Teutio, A. O. N., & Nyongo, A. S. A. (2024). E-Governance, Digitized Tax Procedures and SME's Business Process Performance in Cameroon. *iBusiness*, *16*(3), 65–84. https://doi.org/10.4236/ib.2024.163006

Fang, Z. (2002). E-government in digital era: concept, practice, and development. *International Journal of the Computer, the Internet and Management*, *10*(2), 1–22.

Foster, K. (2020). Smarten Up: Paths to bottom-up smart cities and the risks of top-down smart governance. *Smart Cities Paper Series: Smart Governance in South African Cities*.

Grigalashvili, V. (2022). E-government and E-governance: Various or Multifarious Concepts. *International Journal of Scientific and Management Research*. *5*(01).183–196. https://doi.org/10.37502/ijsmr.2022.5111

Halachmi, A. (2004). E-government theory and practice: The evidence from Tennessee (USA). In M. Holzer, M. Zhang, & K. Dong (Eds.), *Frontiers of Public Administration: Proceedings of the Second Sino-U.S. International Conference: Public Administration in the Changing World* (pp. 24–43). United Nations Public Administration Network.

Heeks, R. (2003). E-Government in Africa: Promise and practice. *Information Polity*, *7*(23), 97–114. https://doi.org/10.3233/ip-2002-0008

Heeks, R. (2006). *Implementation and managing e-Governance*. London: Sage publications Ltd.

Kaisara, G., & Pather, S. (2011). The e-Government evaluation challenge: A South African Batho Pele-aligned service quality approach. *Government Information Quarterly*, *28*(2), 211–221. https://doi.org/10.1016/j.giq.2010.07.008

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In M. E. Compton, & P. Hart (Eds.), *Great Policy Successes* (pp. 143–160). Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008

Lubis, S., Purnomo, E. P., Lado, J. A., & Hung, C. F. (2024). Electronic governance in advancing sustainable development goals through systematic literature review. *Discover Global Society*, *2*(1) 77. https://doi.org/10.1007/s44282-024-00102-3

Makwanya, M. (2022). Digital practice for social work in Zimbabwe: Success, challenges and opportunities. In A. L. Peláez, S. Suh, & S. Zelenev (Eds.), *Digital Transformation and Social Well-Being* (pp. 160–168). Routledge.

Munyoka, W. (2020). Electronic government adoption in voluntary environments–a case study of Zimbabwe. *Information Development*, *36*(3), 414–437. https://doi.org/10.1177/0266666919864713

Muttoo, S. K., Gupta, R., Pal, S. K., & Muttoo, S. K. (2019). *E-Governance in India* (pp. 13–25). Singapore: Springer. https://doi.org/10.1007/978-981-13-8852-1

Naqvi, S. A. M., Alyas, T., Tabassum, N., Namoun, A., & Naqvi, H. H. (2021). Post Pandemic World and Challenges for E-Governance Framework. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2630–2636. https://doi.org/10.30534/ijatcse/2021/1571032021

Oliveira, T. A., Oliver, M., & Ramalhinho, H. (2020). Challenges for Connecting Citizens and Smart Cities: ICT, e-Governance and Blockchain. *Sustainability*, *12*(7), 2926. https://doi.org/10.3390/su12072926

Palvia, S. C. J., & Sharma, S. S. (2007). E-government and e-governance: definitions/domain framework and status around the world. In *International Conference on E-governance* (Vol. 5, No. 1, pp. 1–12).

Prashar, K., & Bawa, S. S. (2023). Studying the Effect of Artificial Intelligence on E-Governance. In P. Tyagi, S. Grima, K. Sood, B. Balamurugan, E. Özen, & T. Eleftherios (Eds.), *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a Global Digitalised Economy (Contemporary Studies in Economic and Financial Analysis, Vol. 110A)* (pp. 87–101). Emerald Publishing Limited, Leeds. https://doi.org/10.1108/S1569-37592023000110A005

Reiling, D., & Contini, F. (2022). E-Justice Platforms: Challenges for Judicial Governance. *International Journal for Court Administration*, *13*(1), 6. https://doi.org/10.36745/ijca.445

Schuppan, T. (2009). E-Government in developing countries: Experiences from sub-Saharan Africa. *Government Information Quarterly*, *26*(1), 118–127. https://doi.org/10.1016/j.giq.2008.01.006

Sevidzem, M. C. (2024). Use of ICT and the Application of E-Governance Strategies in Service Delivery by Local Councils in Cameroon: The Case of Local Councils in the Bamenda Municipality. *PanAfrican Journal of Governance and Development (PJGD)*, *5*(1), 3–27. https://doi.org/10.46404/panjogov.v5i1.5354

Sharma, S., Kumar Kar, A., & Gupta, M. P. (2021). Unpacking Digital Accountability: Ensuring efficient and answerable e-governance service delivery. In *Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance* (pp. 260–269). https://doi.org/10.1145/3494193.3494229

Suri, P. K., & Sushil. (Eds.) (2017). *Strategic Planning and Implementation of E-Governance*, Springer.

Suthar, A. B., Khalifa, A., Yin, S., Wenz, K., Ma Fat, D., Mills, S. L., ... & Mrkic, S. (2019). Evaluation of approaches to strengthen civil registration and vital statistics systems: a systematic review and synthesis of policies in 25 countries. *PLoS Medicine*, *16*(9), e1002929. https://doi.org/10.1371/journal.pmed.1002929

Tammpuu, P., & Masso, A. (2018). 'Welcome to the virtual state': Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies*, *21*(5), 543–560. https://doi.org/10.1177/1367549417751148

Umbach, G., & Tkalec, I. (2022). Evaluating e-governance through e-government: Practices and challenges of assessing the digitalisation of public governmental services. *Evaluation and program planning*, *93*, 102–118. https://doi.org/10.1016/j.evalprogplan.2022.102118

Xin, G., Esembe, E. E., & Chen, J. (2023). The mixed effects of e-participation on the dynamic of trust in government: Evidence from Cameroon. *Australian Journal of Public Administration*, *82*(1), 69–95. https://doi.org/10.1111/1467-8500.12569

Authors information

Robert Kosho Ndiyun – PhD (Political Studies), Post-Doctoral Research Fellow, Department of Public Affairs, Tshwane University of Technology
Address: Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: NdiyunRK@tut.ac.za
ORCID ID: https://orcid.org/0000-0002-6435-0494
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57762430700
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JCD-5501-2023
Google Scholar ID: https://scholar.google.com/citations?user=siNlKWQAAAAJ

Ricky Munyaradzi Mukonza – DTech (Public Management), Associate Professor of Public Management, Department of Public Affairs, Tshwane University of Technology
Address: Staatsartillerie Rd, Philip Nel Park, 0183 Pretoria, South Africa
E-mail: MukonzaRM@tut.ac.za
ORCID ID: https://orcid.org/0000-0001-8121-1501
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56157610200
Google Scholar ID: https://scholar.google.com/citations?user=LXj9QUQAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – January 18, 2025
Date of approval – January 31, 2025
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:347.78:340.13:347.9:004.8
EDN: https://elibrary.ru/ppfjub
DOI: https://doi.org/10.21202/jdtl.2025.2

Эволюция авторского права в эпоху искусственного интеллекта: анализ правовых коллизий и судебных прецедентов

Фемистоклис Цимас

Университет Фракии имени Демокрита, Комотини, Греция

Ключевые слова

авторское право,
законодательство,
интеллектуальная собственность,
искусственный интеллект,
междисциплинарный подход,
право,
правовое регулирование,
суд,
технологический прогресс,
цифровые технологии

Аннотация

Цель: комплексный критический анализ современных проблем в области правового регулирования технологий искусственного интеллекта, возникающих на стыке норм интеллектуальной собственности и искусственного интеллекта. Особое внимание уделяется исследованию коллизий между существующим европейским законодательством об авторском праве и новыми технологическими реалиями.

Методы: в работе применяется междисциплинарный подход, включающий исторический, формально-юридический и сравнительно-правовой методы исследования. Исторический метод позволил проследить эволюцию законодательных и доктринальных подходов к регулированию интеллектуальной собственности в эпоху цифровизации. Формально-юридический метод дал возможность провести детальный анализ правовых норм различных государств. Сравнительно-правовой метод обеспечил возможность сопоставления различных подходов к регулированию отношений, связанных с использованием искусственного интеллекта в творческой деятельности.

Результаты: в ходе исследования детально рассмотрены вопросы авторского права на произведения, созданные с помощью искусственного интеллекта, включая сложные аспекты определения авторства и проблемы антропоцентризма в современном законодательстве. Проведен анализ судебных прецедентов, преимущественно в контексте законодательства Европейского союза, которое активно адаптируется к новым технологическим вызовам. Исследованы различные подходы к определению правового статуса произведений, созданных с помощью искусственного интеллекта, и их влияние на традиционные концепции интеллектуальной собственности.

Научная новизна: в статье впервые представлена комплексная оценка влияния творческих возможностей искусственного интеллекта на

фундаментальные концепции интеллектуальной собственности. Научная значимость заключается в оригинальной авторской оценке воздействия технологий искусственного интеллекта на законодательство об авторском праве, основанной на детальном анализе судебных прецедентов и доктринальных подходов. Исследованы перспективы развития правового регулирования в условиях технологического прогресса.

Практическая значимость: в работе предложены конкретные правовые и государственные решения, направленные на формирование сбалансированного и эффективного режима интеллектуальной собственности в эпоху искусственного интеллекта. Разработаны рекомендации по совершенствованию законодательства с учетом существующих судебных прецедентов и потребностей цифровой экономики. Результаты исследования могут быть использованы при разработке новых нормативных актов и совершенствовании существующей правовой базы в области регулирования искусственного интеллекта.

Для цитирования

Цимас, Ф. (2025). Эволюция авторского права в эпоху искусственного интеллекта: анализ правовых коллизий и судебных прецедентов. *Journal of Digital Technologies and Law*, *3*(1), 35–64. https://doi.org/10.21202/jdtl.2025.2

Содержание

Введение

В быстро меняющейся сфере интеллектуальной собственности интеграция искусственного интеллекта (далее – ИИ) в творческий процесс стала неоспоримо мощным фактором, который изменил саму природу оригинальных произведений и привнес множество сложных юридических аспектов (Greenstein, 2022). Правовые системы пытаются осмыслить преобразующее воздействие ИИ на интеллектуальную собственность[1]. В основе этих эффектов лежит уникальная онтология искусственного интеллекта и, более конкретно, его автономия, которая позволяет ИИ создавать творческие и оригинальные работы без какого-либо или, по крайней мере, критического

[1] Love, J. (2023, August 7). We Need Smart Intellectual Property Laws for Artificial Intelligence, Scientific American. https://clck.ru/3GEWjn ; Ogwuche, Perpetua. (2022, October 16). Artificial Intelligence: The Legal Implications of Intellectual Property Rights for AI-generated Inventions. https://clck.ru/3GEWku

вмешательства человека. Хотя этот юридический вопрос возник совсем недавно, в различных правовых системах по всему миру уже принят ряд судебных решений[2]. В настоящей статье предпринята попытка исследовать взаимосвязь между произведениями, созданными с помощью искусственного интеллекта, и нормами интеллектуальной собственности со ссылкой на соответствующие недавние судебные решения. Цель работы – изучить возможное влияние указанных решений на направление развития законодательства Европейского союза. Точка отсчета – роль антропоцентризма как необходимого условия защиты интеллектуальной собственности.

Рост влияния ИИ на создание защищенных авторским правом, запатентованных и находящихся в собственности произведений имеет ряд последствий. Последствия эти потенциально катастрофичны из-за растущих возможностей ИИ и его способности имитировать характеристики человеческого интеллекта. Эти способности, по крайней мере, напоминают творческие способности и оригинальность мышления человека. Исходя из этого, разумно задаться вопросом о том, кому должны принадлежать изобретения, созданные с помощью искусственного интеллекта, в целом и по законодательству ЕС в частности. В следующем разделе работы мы кратко рассмотрим некоторые элементы онтологии искусственного интеллекта, которые имеют решающее значение для понимания того, почему ИИ бросает вызов антропоцентризму в отношении права интеллектуальной собственности.

1. Онтология искусственного интеллекта и значение его автономии

Закон ЕС об искусственном интеллекте определяет ИИ как «систему, которая предназначена для работы с определенным уровнем автономии и которая, основываясь на информации и входных данных, предоставляемых машиной и/или человеком, определяет, как достичь заданного набора определенных человеком целей, используя машинное обучение и/или подходы, основанные на логике и знаниях, а также выдает сгенерированные системой результаты, такие как контент (генеративные системы искусственного интеллекта), прогнозы, рекомендации или решения, влияющие на среды, с которыми взаимодействует система искусственного интеллекта»[3]. Это определение используется в настоящей статье для того, чтобы избежать частого повторения определения ИИ, а также из-за его всеобъемлющего значения. Оно относится к широкому спектру результатов ИИ, от принятия решений до контента. Именно на основе этой онтологии возникает вопрос о регулировании произведений, создаваемых искусственным интеллектом[4].

Концепция ИИ изначально строится на стремлении создать машины, которые могут имитировать человеческий интеллект или его аспекты; другими словами, развитие ИИ относится к поиску нового типа разумных существ (Gerdes, 2018).

---

2 В статье даются ссылки на важнейшие из них.

3 The EU Artificial Intelligence Act. https://clck.ru/3GEWoH

4 До этой законодательной инициативы Европейская комиссия направила Европейскому парламенту обращение «Искусственный интеллект для Европы», в котором ставились такие цели, как «повысить технологический и промышленный потенциал ЕС и степень использования ИИ в экономике… подготовиться к социально-экономическим изменениям, вызванным созданием надлежащих этических и правовых норм»; EC, “Artificial Intelligence for Europe”, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2018/237 final, 25 April 2018.

Фундаментальным элементом ИИ является его расширяющаяся интеллектуальная автономия, которая обеспечивает ему способность адаптироваться к новым условиям (Omohundro, 2008; Russell & Norvig, 2010). Именно переход от автоматизации к автономии делает ИИ таким уникальным. Автономность означает, что ИИ не является простым результатом заранее определенного программного обеспечения, а имитирует и воспроизводит процедуру обучения человека и аспекты человеческого интеллекта посредством машинного обучения (McCarthy, 2008; Lake et al., 2016). Подход Алана Тьюринга состоял в том, чтобы компьютер мог повторить мышление, методологию и развитие ребенка (Turing, 1950).

Машинное обучение означает, что искусственный интеллект «учат» тому, как выдавать определенные результаты (Bostrom & Ćirkovic, 2008). Цель машинного обучения в аспекте ИИ состоит в том, чтобы достичь естественных закономерностей развития и, следовательно, получать решения для широкого спектра не предопределенных заранее задач без обязательного участия людей (Bostrom, 2014). Таким образом, ИИ учится и принимает решения на основе действий с наибольшей ожидаемой полезностью в свете основных предпочтений и целей (Bostrom, 2014).

«Машинное обучение» происходит на основе сбора и использования больших объемов данных для обучения алгоритмов. ИИ обучается на основе наших общих данных, порожденных всем сообществом, и в этом смысле автономия ИИ по сути (по крайней мере, частично) является социальным результатом. Именно эта процедура дает возможность искусственному интеллекту развивать и демонстрировать такие характеристики, как логика[5] (инструмент анализа[6]), креативность; способность решать задачи, распознавать образы; классифицировать, обучаться, использовать индукцию, дедукцию, построение аналогий, оптимизацию, умения выживать в среде и обрабатывать язык (Hutter, 2010; Hallevy, 2018), самостоятельно совершать когнитивные операции, применять интуицию и стратегическое мышление (Yanisky-Ravid & Liu, 2018; Hallevy, 2018; Suchman & Weber, 2016)[7]. ИИ еще не осознает все эти характеристики, как человек, поскольку не обладает саморефлексивным интеллектом, но во многих областях он уже выдает результаты, которые у человека являются предпосылкой для таких интеллектуальных способностей (Laton, 2016; Russell & Norvig, 2010)[8].

Машинное обучение также объясняет, почему по мере развития ИИ его онтология становится вероятностной, нелинейной, сложной, непрозрачной и, следовательно, непредсказуемой, что приводит к возникновению фундаментальных неопределенностей, которые были описаны как «эффект черного ящика»; мы не можем быть уверены в том, каким будет результат машинного обучения и действий ИИ[9]. Мы знаем входные данные и видим итог машинного обучения,

---

5 Thomason, R. Logic and Artificial Intelligence. Stanford Encyclopedia of Philosophy. https://clck.ru/3GEWqZ

6 Там же.

7 Camett, J. B., & Heinz, E. (2006, Apr 19). John Koza Built an Invention Machine. Popular Science. https://clck.ru/3GEWtB

8 Pyle, D., & San Jose, C. (2015, June). An executive's guide to machine learning. McKinsley Quarterly. https://clck.ru/3GEWuK

9 InFERENCe. (2015, August 13). The Two Kinds of Uncertainty an AI Agent Has to Represent. https://clck.ru/3GEWvd

но мы не уверены в том, что находится между ними (Karppi & Crawford, 2016; Van Asselt & Renn, 2011). Автономность и, как следствие, адаптивность – уникальное преимущество искусственного интеллекта, но именно оно таит в себе значительный риск: ИИ часто остается «черным ящиком» (Castelvecchi, 2016).

Несомненно, существуют серьезные разногласия по поводу того, сможет ли искусственный интеллект достичь прорывов, которые приведут его к уровню общего интеллекта и, главным образом, когда это может произойти[10]. Тем не менее даже нынешняя узкая автономия ИИ дает преобразующие результаты, в частности, в отношении оригинальной интеллектуальной деятельности, что уже значительно ограничивает или сокращает участие человека в этом процессе (Martinez, 2019).

Дискуссия о том, может ли ИИ проявлять творчество и оригинальность или это исключительно человеческие качества, носит междисциплинарный характер и в значительной мере пока остается без ответа (Hashiguchi, 2017b; Hattenbach & Snyder, 2018)[11]. В определенной степени ИИ – по крайней мере, тот, который существует в настоящее время, – просто угадывает закономерности и поэтому никогда не сможет быть творческим и оригинальным. С другой стороны, этот подход очень несправедлив, поскольку он не учитывает, что даже в своей ограниченной форме ИИ эмулирует характеристики человеческого разума, включая аспекты творчества. Частично позволяет обойти это онтологическое противоречие (но также дает на него ответ в области права) тот факт, что независимо от того, считаем мы ИИ онтологически творческим или нет, он создает произведения, которые, если бы были созданы людьми, считались бы творческими и, следовательно, защищались бы нормами авторского права.

Таким образом, алгоритмы создают произведения, которые, будучи созданы человеком, подпадали бы под нормы интеллектуальной собственности. Как закон должен относиться к таким произведениям? Должны ли они охраняться Законом об интеллектуальной собственности в интересах физических или юридических лиц или к ним должен быть свободный доступ (Xu et al., 2018)[12]? В следующем разделе мы кратко рассмотрим основы законодательства в области интеллектуальной собственности в целом и соответствующего законодательства ЕС в частности. Затем мы опишем судебные прецеденты, позволяющие оценить влияние искусственного интеллекта на законодательство в области интеллектуальной собственности в целом и на таковое ЕС в частности.

---

10 Например, и это достаточно показательно, в то время как многие эксперты рассматривают «генеративный ИИ» как уникальный научный прорыв, другие оценивают его низко, говоря, что ИИ всего лишь предсказывает последовательности на основе обширных данных. Хотя мы не можем точно описать, как именно работает человеческий интеллект, он определенно делает «больше», чем генеративный ИИ.

11 Gottschalk v. Benson, 409 U.S. 63, 67 (1972); Hauser, L. Artificial Intelligence. Internet Encyclopedia of Philosophy. https://clck.ru/3GEX2y

12 Schwab, K. (2015). The Fourth Industrial Revolution: What It Means and How to Respond. https://clck.ru/3GEX4J ; Xiang, F. (2018). AI Will Spell the End of Capitalism. Available via The Washington Post. https://clck.ru/3GEX6N ; Acemoglu, D., & Restrepo, P. (2017). Robots and Jobs: Evidence from US Labor Markets. MIT Department of Economics Working Paper, 17-04. https://clck.ru/3GEX7H ; Yongjun, Xu et al. (2021, November 28). Artificial intelligence: A powerful paradigm for scientific research. The Innovation, 2, 100179.

2. Основы норм в области интеллектуальной собственности и влияние искусственного интеллекта. Взгляд с точки зрения законодательства Европейского союза

Чтобы разобраться в законодательстве об ИИ и интеллектуальной собственности (далее – ИС), сначала необходимо кратко рассмотреть основы законодательства об ИС. Прежде всего, интеллектуальная собственность «…в широком смысле означает юридические права, возникающие в результате интеллектуальной деятельности в промышленной, научной, литературной и художественной областях»[13]. Закон об интеллектуальной собственности по своей сути очень прост: он преобразует знания и их практическое применение в экономическую ценность (Manderieux, 2010). Предполагается, что он помогает достичь баланса между конкурирующими частными и государственными интересами и регулирует доступ к льготам (Pila & Torremans, 2019).

С точки зрения законодательства об интеллектуальной собственности научные работы относятся к сфере авторского права, а изобретения – к промышленной собственности[14]. Согласно определению, изобретения представляют собой новые решения технических проблем, в то время как научные открытия состоят в «признании явлений, свойств или законов материальной вселенной, которые ранее не были признаны и которые подлежат проверке»[15]. Базовым элементом интеллектуальной собственности является сочетание творческой, неочевидной, оригинальной идеи или изобретения с их практическим применением в промышленности. Определение соответствия каждому конкретному критерию представляет собой юридическую проблему.

Теоретическими основами норм в области интеллектуальной собственности служат теория труда/бездействия и теория утилитаризма/стимулирования (Khoury, 2017). В первом случае акцент делается на вознаграждении за труд создателя, а во втором – на мотивации создателей к дальнейшей работе над новыми идеями и произведениями (Fisher, 2001)[16]. Обе теории основаны на двух фундаментальных предпосылках: во-первых, каждое охраняемое произведение имеет автора-человека и, во-вторых, этот человек должен получить вознаграждение за свою работу.

Концепция защиты интеллектуальной собственности подвергалась критике на том основании, что нормы в области интеллектуальной собственности не несут социальной пользы, способствуют развитию монополий и, следовательно, препятствуют инновационному развитию (Hemel & Ouellette, 2013; Rai, 1999). Кроме того, права

---

13 World Intellectual Property Organization. (2014). WIPO Intellectual Property Handbook. Согласно Конвенции об учреждении Всемирной организации интеллектуальной собственности (далее – ВОИС), «сфера интеллектуальной собственности включает права, относящиеся к литературным, художественным и научным произведениям; выступлениям артистов-исполнителей, фонограммам и радиопередачам; изобретениям во всех областях человеческой деятельности; научным открытиям; промышленным образцам; товарным знакам, знакам обслуживания, коммерческим наименованиям и обозначениям; право на защиту от недобросовестной конкуренции и все другие права, возникающие в результате интеллектуальной деятельности в промышленной, научной, литературной или художественной областях»; Convention Establishing the World Intellectual Property Organization (as amended on September 28, 1979) (Authentic text). https://clck.ru/3GEX8a

14 Что касается искусственного интеллекта, то законодательство об авторском праве также может быть актуальным, если оно относится к «компьютеризированным системам хранения и поиска информации»; WIPO Intellectual Property Handbook, (2014).

15 World Intellectual Property Organization. (2014). WIPO Intellectual Property Handbook; The Geneva Treaty on the International Recording of Scientific Discoveries, Article 1.

16 United Nations The Role of Patents in the Transfer of Technology to Developing Countries. E. 75. II. D. 6, 1975.

интеллектуальной собственности не возникают, как другие права собственности, из-за ограниченности ресурсов, но сами создают эту ограниченность, которая в конечном итоге приводит к снижению благосостояния, по крайней мере, на уровне социума в целом (Krauss, 1989). Если в обществе сильна концепция всеобщего достояния, она служит «двигателем», открывающим для общества новые идеи и изобретения; в то же время защита интеллектуальной собственности исключает или снижает доступность охраняемых произведений, тем самым ограничивая свободный поток идей и их практическое применение (Cohen, 2006; Salzberger, 2006). Общественное достояние – это «океан», а интеллектуальная собственность – «острова», которые в конечном итоге «растворяются» в океане (Khoury, 2017). Таким образом, права интеллектуальной собственности во всех правовых системах всегда должны быть сбалансированы с более широкими общественными интересами, чтобы избежать злоупотребления этими правами: доступ общественности не может несправедливо ограничиваться в пользу какого-либо физического или юридического лица. Это требование становится еще более критичным, когда речь заходит об ИИ и постепенном вытеснении человека из этой цепочки.

Еще одним общим элементом всех правовых систем является то, что они исключают интеллектуальную деятельность из сферы охраны интеллектуальной собственности. Этот вопрос был прояснен на множестве судебных прецедентов, где проводилось важное различие между умственной деятельностью как таковой и умственной деятельностью, имеющей промышленное применение. В первом случае результаты умственной деятельности не подлежат патентованию. Во втором случае они могут быть запатентованы на основании оценки взаимосвязи между умственной деятельностью и ее промышленным применением[17].

По данным Европейского патентного ведомства, существует четыре основных требования к защите интеллектуальной собственности: «должно существовать ‘изобретение’, ‘пригодное для промышленного применения’, которое является ‘новым’ и имеет ‘изобретательский уровень’»[18]. В правовой системе ЕС именно личность

[17] См. в особенности: (Hashiguchi, 2017a); Elec. Power Group, LLC v. Alstom S.A., 830 F.3d 1350, 1351 (Fed. Cir. 2016), 2351-2359; In re TLI Communications LLC Patent Litigation, 823 F.3d 607-613 (Fed. Cir. 2016); Alice Corp. Pty., 134 S. Ct. at 2354 (citing Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133; Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1339 (Fed. Cir. 2016); Mayo Collaborative Servs. v. Prometheus Labs., 566 U.S. 66, 77 (2012) («Перед нами стоит вопрос, содержится ли в заявке на изобретение нечто большее, чем просто описание этих естественных взаимосвязей. Если говорить более точно, они лишь констатируют наличие корреляций или в них содержится достаточно дополнительной информации, чтобы описываемые процессы можно было квалифицировать как патентоспособные процессы, основанные на законах природы?»); European Patent Office, Convention On The Grant Of European Patents 108; McRO, Inc. v. Bandai Namco Games Am. Inc., 837 F.3d 1299, 1302-1316 (Fed. Cir. 2016); Fitbit Inc. v. AliphCom, No. 16-cv-00118-BLF (N.D. Cal. Mar. 2, 2017) at 10, 22; Decision of the European Patent Office. (2004, Apr. 21). Technical Board of Appeal, Case T 258/03–3.5.1, Reasons for the Decision, 3.3, 3.7, 4.1, 4.3, 4.4, 4.7. https://clck.ru/3HrAYg ; In re Sesame Active System, 15/01962, Cour d'Appel de Paris [Court of Appeal of Paris] (26 fevrier 2016 [Feb. 26, 2016]); In re Dassault Systèmes, 14/06444, Cour d'Appel de Paris [Court of Appeal of Paris] (16 décembre 2016 [Dec. 16, 2016]); (Hashiguchi, 2017b); Decision of the European Patent Office. (1988, Oct. 5). Technical Board of Appeal, Case T 22/85–3.5.1, Reasons for the Decision, 5. https://clck.ru/3HrAYg ; Decision of the European Patent Office. (1995, Jan. 20). Technical Board of Appeal, Case T 0605/93-3.5.1, 5.3, 5.7. Reasons for the Decision, 5.9. https://clck.ru/3HrAYg. Кроме того, нормы интеллектуальной собственности не применяются к изобретениям, использующим законы природы; S. Ct. 2107, 2116 (2013); Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289, 1293 (2012)).

[18] European Patent Office. Patentability requirements. https://clck.ru/3HrAEr ; European Patent Office, Convention on the Grant of European Patents 108 (16th ed., 2016, June). https://clck.ru/3HrAKW (компиляция статей Европейской патентной конвенции).

автора защищена законами об авторском праве[19] (Kur et al., 2013). Личность автора и креативность, которую он демонстрирует, представляют собой синтез, результатом которого является оригинальность произведения (Hugenholtz & Quintais, 2021). Уровень креативности оценивается индивидуально и на основе общих рекомендаций (van Gompel, 2014). Не подвергается сомнению, что в отсутствие личности автора дальнейшая оценка теряет смысл[20].

То, что защита личности автора составляет основу законодательства ЕС об авторском праве, очевидно из целого ряда норм: произведение не может быть изменено или искажено без разрешения автора, независимо от возможного факта передачи авторских прав[21]; оно должно быть связано с именем автора; опубликование произведения без разрешения автора запрещено; автор сохраняет за собой право отозвать свое произведение[22]. Эти элементы, по сути, составляют теоретическую основу естественного права ЕС (Holst, 2006; Adler, 2009).

Согласно законодательству ЕС и в частности решениям Европейского суда, понятие оригинальности увязывается с «собственным интеллектуальным творчеством автора» и, следовательно, по умолчанию – с авторством человека (van Eechoud, 2012). За короткий период времени, с 2009 по 2012 г., Европейский суд вынес пять решений о связи понятий оригинальности и авторства[23]. В этих решениях было разъяснено, что оригинальность заключается в «собственном интеллектуальном творчестве автора», которое предполагает свободный творческий выбор.

---

19 Lundstedt, L. (2016). Territoriality in intellectual property law: a comparative study of the interpretation and operation of the territoriality principle in the resolution of transborder intellectual property infringement disputes with respect to international civil jurisdiction, applicable law and the territorial scope of application of substantive intellectual property law in the European Union and United States: Doctoral dissertation. Stockholm University.

20 Следует подчеркнуть, что ЕС не обладает исключительными полномочиями по разработке законодательства в области интеллектуальной собственности; (Kur et al., 2013); European Commission, Shaping Europe's digital future, The EU copyright; Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs, article 1(3)), Directive 96/9 of 11 March 1996 on the legal protection of databases, article 3(1)), Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights, article 6; Case C-277/10 – Martin Luksan v. Petrus van der Let (2012) ECLI:EU:C:2012:65 (Luksan), para. 59, and Case C-310/17 – Levola Hengelo BV v. Smilde Foods BV (2018) ECLI:EU:C:2018:899 (Levola Hengelo), paras. 38–39 legislation. https://clck.ru/3GEXR2 ; Бернская конвенция, помимо прочего, упрощает процедуры защиты авторских прав, устанавливает минимальный срок охраны и защищает личные неимущественные права авторов; Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as last amended, July 24, 1971 European Commission, Commission adopts Action Plan on Intellectual Property to strengthen EU's economic resilience and recovery. https://clck.ru/3GEXRY

21 (Hansmann & Santilli, 1997). В сфере охраны авторских прав существуют исключения во имя общественных интересов в целях развития науки, образования и культуры, а также в отношении данных и интеллектуального анализа данных, осуществляемого «исследовательскими организациями и учреждениями культурного наследия для проведения научных исследований». The InfoSoc Directive, Art. 5; Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92 -DSM Directive.

22 Там же.

23 Infopaq International v. Danske Dagblades Forening [2009]; Bezpečnostní softwarová asociace v. Ministerstvo kultury [2010]; Football Association Premier League v. QC Leisure and Karen Murphy v. Media Protection Services [2011]; Eva-Maria Painer v. Standard VerlagsGmbH [2011]; Football Dataco v. Yahoo! [2012].

Такого выбора не происходит, когда соответствующие методы, функции или правила требуют от автора выражать свои идеи только одним определенным способом, не оставляя возможностей для свободного выбора. Креативность и свободный выбор – это, по сути, качественные, а не количественные характеристики. Важны не усилия, которые вкладываются в каждое произведение, а уровень креативности, который неотделим от свободы выбора[24]. Это относится как к традиционным произведениям, так и к работам, основанным на новых технологиях[25].

До появления искусственного интеллекта авторство, очевидно, принадлежало человеку. Этот аспект был обусловлен тем фактом, что творчество, как и свобода выбора, предполагает наличие интеллектуальных способностей и, очевидно, является сферой человеческой деятельности[26]. Поскольку право интеллектуальной собственности защищает личность автора, какая личность должна быть защищена, если

---

[24] «Значительные трудозатраты и квалификация, необходимые для создания этой базы данных, сами по себе не могут служить основанием для такой защиты, если они не отражают какой-либо оригинальности в выборе или расположении данных, содержащихся в этой базе» (Football Dataco v Yahoo [2012], 53(1)).

[25] Конкретный необходимый уровень оригинальности определяется каждым государством-членом. Directive 98/71/EC of 13October 1998 on the legal protection of designs, article17; Regulation (EC) No. 6/2002 of 12 December 2001 on community designs, article 96; Computer Programs Directive, recital 8: «Критерии для определения оригинальности компьютерной программы не должны касаться качественных или эстетических достоинств программы». Ramalho, A. (2019). Originality redux: an analysis of the originality requirement in AI-generated works. AIDA, 9; (Ricketson & Ginsburg, 2005); Case C-5/08 Infopaq International A/S v. Danske Dagblades Forening [2009] ECR I-6569, ECLI:EU:C:2009:465, para. 37; Case C-393/09 Bezpecˇnostn softwarova´ asociace – Svaz softwarove´ ochrany v. Ministerstvo kultury [2010], ECR I-13971, ECLI:EU:C:2010:816, para. 45; Joined Cases C-403/08 and C-429/08, Football Association Premier League v. QC Leisure and Karen Murphy v. Media Protection Services Ltd [2011] ECR I-09083, ECLI:EU:C:2011:631, para. 97; Guide to the Berne Convention (1978), 17–18; (Hutukka, 2023).

[26] Степень креативности варьируется в различных правовых системах, при этом порог может быть выше (как, например, в США) или ниже в зависимости от правовой системы и традиций. Решение по делу Painer о фотопортрете гласило, что автор «может делать свободный и творческий выбор несколькими способами и на различных этапах создания произведения. <…> Делая различные выборы, автор портретной фотографии может придать созданному произведению ‘индивидуальность’. Следовательно, что касается портретной фотографии, то свобода, предоставляемая автору в реализации его творческих способностей, не обязательно будет незначительной или даже вовсе отсутствующей». В деле Cofemel суд постановил, что «для того, чтобы произведение можно было рассматривать как оригинальное, необходимо и достаточно, чтобы оно отражало личность его автора как выражение его свободного творческого выбора». Feist Publications v. Rural Telephone Service 499 U.S. 340 (1991), 346; CCH Canadian v. Law Society of Upper Canada [2004] 1 S.C.R. 339; Case C-145/10 – Painer, paras. 90–93; Case C-145/10 – Painer, para. 92; Case C-683/17 – Cofemel, para. 30; Case C-5/08 Infopaq International A/S v. Danske Dagblades Forening [2009] ECR I-6569; ECLI:EU:C:2009:465, para. 37; Case C-393/09 Bezpecˇnostnı´ softwarova´ asociace - Svaz softwarove´ ochrany v. Ministerstvo kultury [2010], ECR I-13971, ECLI:EU:C:2010:816, para. 45; Joined Cases C-403/08 and C-429/08, Football Association Premier League v. QC Leisure and Karen Murphy v. Media Protection Services Ltd. [2011] ECR I-09083, ECLI:EU:C:2011:631, para. 97; Case C-604/10 Football Dataco and Others v. Yahoo! UK Ltd. and Others[2012]; ECLI:EU:C:2012:115, para. 38; Case C-5/08 Infopaq International A/S v. Danske Dagblades Forening [2009] ECR I-6569, ECLI:EU:C:2009:465, para. 45; Case C-393/09 Bezpecˇnostnı´softwarova´ asociace - Svaz softwarove´ ochrany v. Ministerstvo kultury [2010], ECR I-13971, ECLI:EU:C:2010:816, para. 50; Case C-145/10 Eva-Maria Painer v. Standard VerlagsGmbH and Others [2011] ECLI:EU:C:2011:798,paras. 89, 92; отметим, что под оригинальностью понимается состояние, при котором работа не является копией, но представляет собой результат «мастерства, суждения и/или работы» (Bently & Sherman, 2014).

автора-человека нет?[27] Теперь в эти отношения вступает искусственный интеллект, и все эти самоочевидные до недавнего времени факты проверяются с точки зрения его влияния.

Как уже говорилось, развитие технологий привело к фундаментальному пересмотру традиционной концепции авторства еще до появления искусственного интеллекта. Начиная с Зеленой книги 1988 г. и заканчивая Директивой 91/250/EEC от 14 мая 1991 г. о правовой охране программного обеспечения вопрос авторства человека постепенно становится предметом дискуссий (Walter & von Lewinski, 2010). До появления искусственного интеллекта не было особых сомнений в антропоцентризме авторства. Компьютеры – это «автоматы», но не автономные устройства. Однако ИИ, благодаря разнообразным приложениям, может выполнять такую работу, которая до эпохи ИИ могла быть результатом только человеческого интеллекта (Hugenholtz & Quintais, 2021). Даже существующий в настоящее время слабый искусственный интеллект (Artificial Narrow Intelligence, ANI) может создавать произведения практически во всех сферах человеческого творчества и интеллектуальной деятельности (Senftleben & Buijtelaar, 2020; Gervais, 2019; Senftleben & Buijtelaar, 2020; Butler, 1982).

Учитывая, что участие человека в процессе создания снижается, линейная причинно-следственная связь между человеческим «разумом», стоящим за алгоритмом искусственного интеллекта, и конечным изобретением или работой сублимируется, по крайней мере, в значительной степени, а возможно, уже и полностью. Как же оценить этот факт, чтобы решить, следует обеспечивать защиту авторских прав или нет (Hashiguchi, 2017a)? Когда вознаграждение человека за произведение, созданное искусственным интеллектом, уже становится несправедливым (Spector, 2006; Jaszi, 1992; Grinmelmann, 2016)[28]?

---

[27] Например, см. дело InfoSoc относительно юридических лиц, которое рассматривал Европейский суд. Еще более четко эту позицию выразила генеральный адвокат Trstenjak в деле Painer, напрямую связав нормы интеллектуальной собственности с человеком: «Таким образом, защищены только творения человека...»; Case C-277/10 – Luksan; Case C-572/13 – Hewlett-Packard Belgium SPRL v. Reprobel SCRL (2015); ECLI:EU:C:2015:750 (Reprobel); Opinion AG Trstenjak in Case C-145/10 – Painer, para. 121. Того же подхода придерживается Бюро по вопросам авторского права в США: «Произведения, созданные машиной или посредством простого механического процесса, который действует случайным образом или автоматически без какого-либо творческого вклада или вмешательства автора-человека»; USPTO, Compendium of U.S. Copyright Office Practices § 101 (3rd edn. 2017). https://clck.ru/3GEXSn , Arts. 306 and 313(2).

[28] Sloman, A. (2007). What is Artificial Intelligence?, School of Computer Science The University of Birmingham. https://clck.ru/3Hr9gj ; Burrow-Giles Lithographic Co. v. Sarony, Ill U.S. 53 (1884); Midway Mfg. Co. v. Artic Intern., Inc., 704 F. 2d 1009, 1011 (7d Cir. 1983). Еще в 1965 году в США Реестр авторских прав представил Конгрессу отчет о работах, сгенерированных компьютером, в котором поднимался вопрос об авторском праве. Созданная в то время Национальная комиссия по новым технологиям использования произведений, охраняемых авторским правом, постановила, что компьютеры ничем не отличаются от фотоаппаратов или пишущих машинок, а авторские права должны принадлежать только пользователю. U.S. COPYRIGHT OFFICE, SIXTY-EIGHTH ANNUAL REPORT OF THE REGISTER OF COPYRIGHTS 5 (1965). https://clck.ru/3GEo8C ; NAT'L COMM'N ON NEW TECH. USES OF COPYRIGHTED WORKS, FINAL REPORT OF THE NATIONAL COMMISSION ON NEW TECHNOLOGICAL USES OF COPYRIGHTED WORKS 44-45 (1978). https://clck.ru/3GEXrV ; Arsheeya Bajwa. IBM beats profit estimates as AI shift boosts software performance, shares surge. (2025, January 30). Reuters. https://clck.ru/3HK9es ; van den Oord, A., et al. (2016, Sept. 8). WaveNet: A Generative Model for Raw Audio. arXiv. https://clck.ru/3HK9hP ; Mordvintsev, A. et al. (2015, June 17). Inceptionism: Going Deeper into Neural Networks, GOOGLE RES. BLOG. https://clck.ru/3HK9ip ; (Hashiguchi, 2017a).

В этом контексте ряд международных судебных решений помогают лучше проработать наш подход к влиянию искусственного интеллекта на требование, что автор должен быть защищен в соответствии с законодательством об интеллектуальной собственности.

3. Судебные прецеденты, в которых оценивается влияние искусственного интеллекта на законодательство об авторском праве

Соответствующие судебные прецеденты существуют как в государствах – членах ЕС, так и на международном уровне. Их изучение поможет прояснить взаимосвязь между ИИ и защитой интеллектуальной собственности в целом и в соответствии с законодательством ЕС.

Так, в США окружной суд Колумбии постановил, что художественное произведение, полностью созданное с помощью искусственного интеллекта без какого-либо участия человека, не подлежит защите авторским правом из-за отсутствия авторства человека. Дело было возбуждено после того, как владелец компьютерной системы под названием Creativity Machine потребовал зарегистрировать для защиты авторских прав изображение, созданное искусственным интеллектом, а затем передать ему авторские права, поскольку он являлся владельцем системы. Управление по вопросам авторских прав США отказало в защите авторских прав из-за отсутствия авторства человека. Истец сослался на доктрину «наемного труда» общего права. Суд постановил, что этот аргумент относится к «тому, на кого должны быть зарегистрированы действующие авторские права, т. е. ставит телегу впереди лошади». Далее решение суда гласит, что «авторское право должно адаптироваться в соответствии с требованиями времени. Однако эта адаптивность должна основываться на последовательном понимании того, что обязательным условием соблюдения авторских прав является человеческое творчество, даже если оно реализуется посредством новых инструментов или новых средств массовой информации»[29].

В другом деле Управление по вопросам авторских прав США пришло к выводу, что заявка на регистрацию контента, созданного с помощью искусственного интеллекта, не содержит информации о подготовке или идентификации произведения, а также о существовании, владении или сроке действия авторских прав. Поэтому в регистрации произведения, сгенерированного ИИ, было отказано в соответствии с нормами авторского права. В частности, было установлено, что «доля контента, сгенерированного искусственным интеллектом (ИИ), в произведении превышает минимальную, и этот контент не может фигурировать в заявке на регистрацию»[30]. Оцениваемая работа подверглась улучшению человеком, заявившим о защите авторских прав, но комиссия установила, что защита авторских прав не может быть обеспечена, поскольку указанное лицо отказалось исключить из заявки материалы, созданные ИИ, и их доля превысила допустимый минимум объема контента, сгенерированного ИИ. Решение комиссии подтвердило вывод по делу Thaler v. Perlmutter о том, что «авторство человека является основополагающим требованием авторского

[29] US District Court For The District Of Columbia, Stephen Thaler v Shira Perlmutter, Case 1:22-cv-01564-BAH Document 24 Filed 08/18/23, at pp. 7, 8.

[30] United States Copyright Office, Second Request for Reconsideration for Refusal to Register Théâtre D'opéra Spatial (SR # 1-11743923581; Correspondence ID: 1-5T5320R), (2023, September 5).

права»[31]. Комиссия сослалась также на другое известное дело, Urantia Found v. Kristen Maaherra. В нем суд постановил: «чтобы Библия была защищена авторским правом, в ней должен присутствовать какой-то элемент человеческого творчества», но «законодательство об авторском праве не предназначено для защиты творений божественных существ»[32].

Управление по вопросам авторских прав США последовательно придерживается мнения, что авторство человека является фундаментальным требованием для защиты авторских прав. В соответствии с этим подходом оно выпустило официальное руководство, согласно которому основной вопрос заключается в том, «является ли рассматриваемая работа преимущественно произведением человеческого авторства, а компьютер [или другое устройство] выступают лишь вспомогательным инструментом или же традиционные элементы авторства (литературное, художественное или музыкальное произведение или его элементы, их компоновка и т. д.) были задуманы и выполнены не человеком, а машиной»[33].

Управление по патентам и товарным знакам США (United States Patent and Trademark Office, USPTO) выпустило Руководство по изобретениям с использованием искусственного интеллекта, вступившее в силу 13 февраля 2024 г., которое устанавливает правила совместной работы человека и ИИ над изобретениями с использованием искусственного интеллекта. В тех случаях, когда человек и генеративный ИИ играют важную роль в создании изобретения, они считаются соавторами. Однако ИИ не может получить защиту как изобретатель, поэтому ключевым становится вопрос, указано ли в данной патентной заявке «по крайней мере, одно физическое лицо», внесшее «значительный вклад в изобретение». Только в этом случае заявка будет удовлетворять критериям совместного изобретательства Pannu, которые необходимы для установления авторства. Если же она не удовлетворяет этим критериям, то изобретение не может быть запатентовано, поскольку в заявке не указан ни один изобретатель»[34].

Таким образом, для обеспечения защиты интеллектуальной собственности в рамках совместной работы человека и ИИ человек – соавтор изобретения должен доказать, что он одновременно и в решающей степени участвовал как в разработке концепции, так и в промышленном применении изобретения, а не только в одном из этих двух аспектов. Рекомендации USPTO особенно полезны в таких случаях, как, например, когда человек просто выступает владельцем системы искусственного интеллекта и ставит ей задачи для решения. Результат таких действий не подпадает под защиту интеллектуальной собственности. Напротив, проектирование, создание и обучение ИИ для решения конкретной задачи, а также активное участие человека в процессе такого решения могут привести к признанию авторства изобретателя[35].

---

31 Там же.

32 Там же.

33 Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16,190, 16,192 (Mar. 16, 2023) (“AI Registration Guidance”).

34 Факторы Панну (Pannu) включают: значимый вклад в разработку концепции и материализацию изобретения, значимый качественный вклад и оригинальность/креативность; последнее понятие состоит в том, чтобы выйти за пределы простого объяснения известных концепций. Katsulis, A. (2024, May 14). Clarifying AI and inventorship: USPTO’s guidance for AI-assisted inventions. Inside Tech Law. https://clck.ru/3GEY7Q

35 Там же.

Вышеупомянутые руководящие принципы совпали с прецедентом по делу Thaler v Vidal, в котором суд отказал в признании ИИ автором изобретения[36].

Значительный вклад в вопросы ИИ и интеллектуальной собственности внесли решения судов и органов власти США: изобретения, основанные на ИИ, в принципе исключены из сферы охраны интеллектуальной собственности. Речь идет не о фактической способности ИИ изобретать, а о его потенциальной защите в соответствии с законодательством об интеллектуальной собственности. Такая защита возможна только после тщательного количественного и качественного анализа каждого индивидуального случая, оценки роли человеческого фактора и работы искусственного интеллекта[37].

Интернет-суд Пекина частично дистанцировался от вышеупомянутой аргументации в аналогичном деле[38]. Суд провел количественную оценку взаимосвязи между работой человека и ИИ, но пришел к выводу, что произведение подлежит защите авторским правом, поскольку является оригинальным. Его оригинальность обусловлена «использованием многочисленных положительных и отрицательных промптов, а также корректировок, внесенных пользователем для выбора итогового изображения, соответствующего его ожиданиям»[39]. Суд постановил, что, несмотря на участие искусственного интеллекта, изображение, созданное с его помощью, «отражает индивидуальную креативность истца и его эстетический выбор, сделанный в процессе создания». Творческий интеллектуальный вклад истца включал в себя разработку дизайна, выбор промптов, настройку параметров во время создания изображения, внесение изменений и корректировку итогового изображения несколько раз, пока он не получил окончательное изображение, соответствующее его ожиданиям. В свете вышеизложенного суд пришел к выводу, что «модели искусственного интеллекта не обладают правосубъектностью, и люди остаются создателями произведений, выполненных с использованием этой технологии»[40].

Европейский суд пришел к довольно спорному выводу в этом отношении. С одной стороны, он поддерживает оценку степени влияния человеческого интеллекта на производимую работу в каждом конкретном случае, но с другой – он значительно снизил порог необходимого участия человека. Таким образом, хотя это и не отрицает предпосылку авторства человека в принципе, но существенно снижает ее значение. Кроме того, тот факт, что ИИ не обладает правосубъектностью, не должен означать, что авторское право автоматически переходит к его владельцу-человеку. Проблематичность снижения порога необходимого участия человека становится понятной на основе важнейшего принципа защиты интеллектуальной собственности,

---

36 Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022).

37 Канадское ведомство по вопросам интеллектуальной собственности (Canadian Intellectual Property Office, CIPO) пошло по аналогичному пути, но несколько двусмысленным образом. С одной стороны, оно постановило, что ИИ не может быть изобретателем, а с другой – предоставило лазейку, предложив заявителю подать заявление от имени системы искусственного интеллекта и идентифицировать себя как ее законного представителя ИИ.

38 US and Chine pioneer in the evolution of AI. Their Courts' decisions therefore are points of reference.

39 European Union Intellectual Property Office. (2024, May). Recent European Case-Law On The Infringement And Enforcement Of Intellectual Property Rights, at pp. 5–6.

40 Там же, at p. 5.

касающегося личности человека, о чем, в частности, свидетельствует недавнее дело Lithoss Nv vs Vimar S.P.A. and Vecolux B.V.[41] В доводах Пекинского суда, по-видимому, ошибочно путают автоматизацию и автономию. Кроме того, возможна своеобразная «манипуляция» истинной онтологией ИИ с целью не поставить под угрозу защиту интеллектуальной собственности и получение прибыли в будущем.

Тем не менее китайские суды также принимают решения, которые в большей степени соответствуют целям норм в области прав интеллектуальной собственности и их возникновению в результате авторства человека. Так, интернет-суд Пекина постановил в деле Beijing Film Law Firm vs Beijing Baidu Netcom Science & Technology Co Ltd (Film), что создание произведения физическими лицами является необходимым условием для защиты в соответствии с китайским законодательством об авторском праве. В этом случае произведение, созданное ИИ, не должно охраняться законом об авторском праве, независимо от его оригинальности (Yong & Hongxuyang, 2021).

Не во всех государствах законы об авторском праве и судебные прецеденты следуют той же логике, что и в США и ЕС, или, по крайней мере, это происходит не всегда. Так, Великобритания, Южно-Африканская Республика, Новая Зеландия, Ирландия и Индия признали возможность защиты авторских прав на произведения, созданные компьютером без какого-либо вмешательства человека. Согласно решению Высокого суда Англии и Уэльса (High Court of Justice), комбинированные кадры в видеоигре, созданные компьютерной программой, являются произведениями компьютера, поскольку программное обеспечение создает их путем наложения цифровых изображений шаров и кия на изображение бильярдного стола[42]. «В случае литературного, драматического, музыкального или художественного произведения, созданного с помощью компьютера, автором считается лицо, которое принимает необходимые действия для создания произведения»[43]. Хотя суды Великобритании в некоторой степени снижают уровень защиты авторских прав в вышеупомянутых делах и, соответственно, последующую выгоду от защиты авторских прав, тем не менее в этом случае была применена юридически и этически неоправданная норма, т. е. прибыль и право собственности были присуждены людям, которые не доказали своего реального авторства. Такой подход представляет собой нарушение как норм и прав интеллектуальной собственности, так и отношений между работодателем и работником, учитывая, как упоминалось ранее, что машины – это не работники, а принадлежащая кому-то технология, т. е. часть капитала (Hristov, 2017).

Тем не менее в деле Comptroller-General of Patents, Designs and Trade Marks vs Emotional Perception AI Ltd Апелляционный суд Англии отменил предыдущую аргументацию и постановил, что искусственная нейронная сеть (Artificial Neural Network, ANN) не является патентоспособной. Суд рассмотрел три вопроса: является ли ANN «компьютером»? Если это компьютер, то является ли ANN программой для компьютера «как таковой» по смыслу раздела 1(2) Закона о патентах 1977 г. (это означает, что она будет исключена из сферы патентоспособности, если следующий пункт

41 Antwerp Court of Appeal, 2021/AR/1900, LITHOSS NV v VIMAR S.p.A. and VECOLUX BV [13 September 2023].

42 Nova Productions v. Mazooma Games, [2006] EWHC 24 (Ch) (UK).

43 Copyright, Designs, and Patents Act 1988, c.48 §§ 12(7), 79(2), 81(2).

также окажется неприменимым)? Если ANN является программой для компьютера, то можно ли тем не менее исключить ее из числа компьютерных программ (и, следовательно, запатентовать), поскольку она внесла «технический вклад», выходящий за пределы этой программы?»[44] Суд пришел к выводу, что ANN – это компьютер, функционирующий как компьютерная программа, и его рекомендации носят не технический, а эстетический характер. В этом смысле Апелляционный суд «внес поправку» в прецедент Высокого суда, постановив, что произведения, созданные с помощью искусственного интеллекта, не могут получить защиту по законодательству об интеллектуальной собственности.

Федеральный суд Австралии в деле Thaler 2022 г. также пришел к выводу, что ИИ не может быть признан автором изобретения[45]. Суд постановил, что только физические лица могут быть названы «изобретателями» и что необходимо наличие юридических отношений между изобретателем-человеком «…и лицом, впервые получившим право на грант, что юридически невозможно в… случае, когда предполагаемый изобретатель не является юридическим лицом и, следовательно, не может влиять на выполнение задания»[46].

Федеральный суд Германии (Bundesgerichtshof, BGH) по делу DABUS принял важное решение, хотя и с сомнительным силлогизмом. Согласно этому решению, только физические лица могут считаться изобретателями в соответствии с Законом о защите интеллектуальной собственности. Немецкий суд пришел к трем важным выводам. Во-первых, ИИ не может быть изобретателем. Во-вторых, каждое изобретение, созданное ИИ, основано на человеческом вкладе определенного уровня, который, даже если не является изобретательским или существенным, позволяет считать человека автором изобретения при условии, что именно он обладает решающим влиянием. В-третьих, патентная заявка не должна содержать противоречивых утверждений, но должна четко указывать, было ли изобретение создано человеком или искусственным интеллектом[47]. Это решение имеет основополагающее значение, но в то же время вызывает недоумение у определенной части судебной системы. На самом деле именно поэтому оно и имеет основополагающее значение.

Суд перепутал признание ИИ в качестве изобретателя в соответствии с законодательством об интеллектуальной собственности с фактической способностью создавать изобретения. В этом смысле он перепутал право с онтологией. Реальная способность ИИ создавать изобретения почти не подвергается сомнению. Однако суд в своем решении, по-видимому, попытался проигнорировать эту способность ИИ, лишить ИИ реальной способности изобретать, а затем на основании вышеуказанной ложной концепции приписать авторство человеку, даже если его фактическое участие второстепенно или незначительно. Суд утверждает, что достаточно лишь формального упоминания человека в качестве изобретателя. Эта попытка

---

44 Maloshchinskaia, P. (2024, July). Artificial intelligence: English Court of Appeal decides artificial neural network is not patentable. Inside Tech Law. https://clck.ru/3GEY92

45 Commissioner of Patents v Thaler [2022] FCAFC 62 (Thaler FC).

46 O'Brien, J., & Taylor, I. (2022, May 5). Demise of the machines: Full Court of the Federal Court of Australia overturns ruling on AI as a patent 'inventor'. Inside Tech Law. https://clck.ru/3GEYAf

47 Kalhor-Witzel, R. (2024, July). Germany: AI cannot be named as inventor – insights from the Bundesgerichtshof's DABUS decision, Norton Rose Fulbright. https://clck.ru/3GEYCa

придерживаться традиционного подхода к праву интеллектуальной собственности, не принимая во внимание происходящие изменения, приводит к злоупотреблению правами и несправедливому ограничению доступа общественности к преимуществам искусственного интеллекта. Проблема заключается не в том, что суд не признает ИИ автором изобретения в соответствии с законодательством об интеллектуальной собственности, а в том, что он настаивает на признании таковым человека независимо от фактической роли последнего в изобретении. Результатом такого подхода является ограничение доступа общественности к изобретению, хотя на самом деле нет человеческой личности, нуждающейся в защите. В этом смысле это решение противоречит подходу законодательства ЕС, ориентированному на естественное право, которое утверждает необходимость защиты личности человека, действительно создавшего нечто оригинальное благодаря своему творческому мышлению.

Чешский суд вынес историческое решение, соответствующее требованию об авторстве человека. Дело рассматривалось муниципальным судом Праги. Истец использовал программу искусственного интеллекта DALL-E для создания изображения по запросу: «Создать визуальное изображение двух сторон, подписывающих деловой контракт в официальной обстановке, такой как конференц-зал или офис юридической фирмы в Праге; показать руки»[48]. Изображение было использовано истцом на его веб-сайте, а затем скопировано и опубликовано ответчиком без его разрешения. Истец не оспаривал, что изображение создал искусственный интеллект, но утверждал, что должен быть защищен авторским правом как лицо, поставившее задачу для ИИ. Суд отклонил его доводы, приняв решение о том, что, во-первых, ИИ не может быть признан автором, а во-вторых, в действиях истца не было уникального творческого начала. Пражский суд весьма категорично постановил, что работа, созданная с помощью искусственного интеллекта, не является «произведением», поскольку она не является уникальным результатом творческой концепции физического лица. Согласно решению суда, «авторское право – это абсолютное право, принадлежащее физическому лицу. Если изображение, о котором идет речь, было создано не лично заявителем, а искусственным интеллектом, оно по определению не может быть произведением, защищенным авторским правом»[49].

Вся вышеприведенная судебная практика, несмотря на свои внутренние противоречия, наглядно демонстрирует то, как изобретения, ориентированные на ИИ или созданные ИИ, влияют на международные нормы в области интеллектуальной собственности, и в частности, на нормы законодательства ЕС. Первый и основополагающий момент заключается в том, что защита авторских прав гарантируется исключительно авторам-людям. Это непреходящая и общая международная основа права интеллектуальной собственности. Характерным в этом отношении является прецедент, возникший до эры искусственного интеллекта в деле Burrow-Giles Lithographic Co. v. Sarony, в котором суд постановил, что решающим фактором для защиты авторских прав является оригинальность идей автора. Определение термина «автор», по мнению суда, является антропоцентрическим, поскольку авторское право характеризуется как «исключительное право человека на продукт своего собственного

[48] Czech court finds AI tool cannot be an author of a copyright work. https://goo.su/MQNOed

[49] Novagraaf Team. (2024, May 1). AI and copyright: First ruling from a European court, Novagraaf. https://clck.ru/3GEYFv

гения или интеллекта»[50]. Этому определению следовали как в эпоху автоматизации, так и в эпоху автономии, т. е. в эпоху искусственного интеллекта.

Главный вопрос заключается в том, может ли физическое лицо быть защищено как автор произведения, созданного с помощью искусственного интеллекта. Здесь можно найти различные подходы. Общая черта прецедентного права из разных правовых систем заключается в том, что авторское право не признается автоматически за физическим лицом, владеющим системой искусственного интеллекта. В некоторых правовых системах, главным образом в США и ЕС, существует требование о существенном вкладе физического лица в изобретение как с точки зрения его концепции, так и с точки зрения его промышленного применения. Только в этом случае он может быть признан в качестве соавтора изобретения. В других правовых системах, как мы уже отмечали, защиту интеллектуальной собственности можно обеспечить даже при минимальном участии физического лица. Однако в любом случае оценка степени участия человека, независимо от того, требуется ли более высокий или более низкий уровень вклада, также является общей для различных правовых систем.

Чтобы оценить роль этих судебных прецедентов в прояснении позиции законодательства ЕС, мы должны иметь в виду, что защита авторских прав в соответствии с законодательством ЕС основана на теориях естественного права. Защита интеллектуальной собственности существует не в силу умозрительных причин, а для материального вознаграждения личности автора и, более конкретно, его творчества. При отсутствии этого элемента не существует моральной и правовой основы для защиты авторских прав в целом и особенно в соответствии с законодательством ЕС (Sobel, 2017). В принципе, нет никакого смысла защищать творения, созданные искусственным интеллектом, в соответствии с нормами интеллектуальной собственности. Передача физическому лицу прав на произведение, которое не включает в себя его творческие способности, представляет собой нарушение норм интеллектуальной собственности, поскольку физическое или юридическое лицо будет извлекать выгоду, ограничивая доступ широкой общественности к произведению, автором которого не является человек.

Чтобы еще лучше понять, насколько несбалансированным и непропорциональным является присвоение таких прав, необходимо также учитывать роль машинного обучения, которое в значительной степени превращает искусственный интеллект в социальный проект, учитывая, что машинное обучение проводится на основе коллективных больших данных, создаваемых всеми нами.

Кроме того, нормы в области интеллектуальной собственности по определению не предназначены для того, чтобы создавать ситуацию «курицы, несущей золотые яйца», или непропорционально ограничивать доступ и интересы общественности. Право интеллектуальной собственности предназначено для защиты творческого потенциала каждого конкретного человека-автора, позволяющего создавать оригинальные произведения с промышленным применением как «острова» в «океане» общедоступных знаний и приложений.

Определение креативности в законодательстве ЕС также заслуживает внимания в сочетании с вышеупомянутыми судебными прецедентами. Европейский суд по правам человека говорит о «…творческих способностях [автора] в создании

[50] Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 54, 56, 58, 61 (1884).

произведения путем осуществления свободного и креативного выбора»[51]. Слово «свободный» подразумевает «автономию». С такой точки зрения ИИ уже может, по крайней мере до некоторой степени, делать выбор, который, если бы его делал человек, считался бы свободным выбором и, следовательно, был бы творческим. В этом случае нет никакого человеческого творчества, которое должно вознаграждаться (Ginsburg & Budiardjo, 2019). Есть только творчество ИИ, которое исключено из сферы защиты интеллектуальной собственности.

Попытка «обойти» факт отсутствия участия человека является одним из аргументов в пользу пересмотра определения понятий работодателя и работника (Hristov, 2017). В соответствии с этим подходом отношения между человеком – владельцем ИИ и самим ИИ рассматриваются как своего рода отношения между работодателем и работником. Однако проблема сохраняется: не существует личности человека, которая была бы основным, а тем более единственным автором произведения, защищенного авторским правом, и, следовательно, ничто не подлежит защите в соответствии с нормами охраны интеллектуальной собственности. Защита авторских прав независимо от отсутствия автора-человека представляла бы собой просто злоупотребление этим правом. Все очень просто: основы защиты авторских прав на произведения, созданные с помощью искусственного интеллекта, отсутствуют, поскольку невозможно определить личность автора-человека. Авторское право представляет собой антропоцентрическую концепцию (Zurth, 2021). В суде США рассматривалось характерное дело по поводу авторских прав на фотографию, на которую кликнула обезьяна. В решении было очень четко указано, что только авторство человека может быть защищено Законом об авторском праве: «Мы приходим к выводу, что эта обезьяна – как и все животные, поскольку они не являются людьми, – не имеет законного статуса в соответствии с Законом об авторском праве»[52].

Более того, наделение машин статусом наемных работников является простым произволом. Все типы машин, по крайней мере до тех пор, пока они не достигнут уровня развития общего или сверхинтеллекта или уровня, эквивалентного уровню полностью автономного юридического лица, рассматриваются как часть капитала. Европейский суд также поддержал вышеупомянутый подход: необходимым условием защиты авторских прав является проявление автором «творческих способностей при создании произведения путем свободного и творческого выбора»[53]. Свободный и творческий выбор делает не владелец ИИ, а тот, кто генерирует идею и создает оригинальную работу.

В конце концов, согласно законодательству ЕС и прецедентам Европейского суда, нет никаких сомнений в связи между личностью автора и интеллектуальной собственностью; любое произведение считается оригинальным, если оно является

51 Case C-469/17 – Funke Medien, para. 19; Case C-145/10 – Painer, paras. 87–88.

52 Naruto v. Slater, 888 F.3d 418, 420 (9th Cir. 2018)").

53 Case C-145/10, Painer v. Standard VerlagsGmbH, 2011 E.C.R. I-12594, 89; see also Case C-604/10, Football Dataco Ltd. v. Yahoo! UK Ltd., ECLI:EU:C:2012:115, 38 (Mar. 1, 2012).

«собственным интеллектуальным творением автора»[54]. Даже профессиональные навыки и труд являются второстепенными по сравнению с элементом «печати личности». Сами по себе они не могут служить основанием для охраны, но являются элементами более широкой системы защиты интеллектуальной собственности[55]. Потенциальная защита работ, созданных ИИ, в соответствии с Законом об авторском праве представляет собой нарушение принципа alterum non laedere («не навреди»): доступ общественности к преимуществам ИИ будет ограничен без каких-либо справедливых и законных оснований для этого. Такой подход является как непропорциональным, так и неразумным (Sganga & Scalzini, 2017; Mizaras, 2012). Чтобы применять нормы интеллектуальной собственности, они должны быть актуальными в каждом конкретном случае, пропорциональными и справедливыми[56]. Очевидно, что этого не происходит, когда отсутствует один из фундаментальных столпов интеллектуальной собственности – автор-человек. Все вышесказанное подводит нас к одному и тому же выводу: Закон об авторском праве антропоцентричен (Ginsburg, 2018).

Однако тот факт, что работы, созданные искусственным интеллектом, не подлежат защите авторского права, не полностью проясняет вопрос о требуемом пороговом значении вклада человека, чтобы он считался их автором или соавтором. Другими словами, более сложный вопрос заключается в том, можем ли мы установить какой-либо качественный и количественный критерий того, когда участие ИИ становится настолько значительным, что человек больше не может считаться автором произведения, потенциально охраняемого авторским правом.

Как было показано выше, вопрос о пороге человеческого вклада находится в процессе обсуждения. Как уже упоминалось, законодательство ЕС в этой области ориентировано на естественное право. Следовательно, правовую систему ЕС следует интерпретировать как стремящуюся установить максимально высокий порог человеческого вклада для обеспечения защиты авторских прав. Такой подход согласуется с решением судов ЕС и США. Личность автора должна быть напрямую связана с изобретением либо в том смысле, что он является единственным изобретателем, либо в качестве соавтора. Это означает, что, например, недостаточно просто задать вопрос ИИ, необходимо, чтобы ИИ выполнял какую-то второстепенную работу или, по крайней мере, чтобы человек творчески перестроил и скомбинировал результаты работы ИИ.

---

54 Infopaq International v. Danske Dagblades Forening [2009]; C393/09 Bezpečnostní softwarová asociace v. Ministerstvo kultury [2010] E.C.R. I-13971; C-403/08 and C-429/08 Football Association Premier League and Others v. QC Leisure and Others and Karen Murphy v. Media Protection Services [2011]E.C.R. I-09083; C-145/10 Eva-Maria Painer v. Standard VerlagsGmbH and Others [2011] E.C.R I-12533; C-604/10 Football Dataco v. Yahoo! UK and Others [2012] EU:C:2012:115) Football Dataco v Yahoo [2012], 53 (1): «Значительные трудозатраты и квалификация, необходимые для создания этой базы данных, сами по себе не могут служить основанием для такой защиты, если они не отражают какой-либо оригинальности в выборе или расположении данных, содержащихся в этой базе».

55 Directive 2009/24, of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs, art. 1, 3, 2009 O.J. (L 111) 16, 18 (EC).

56 Productores de Música de España (Promusicae) v Telefónica de España SAU, Case C-275/06, [2008] ECR I-271, para. 68. Football Association Premier League Ltd and Others v QC Leisure and Others, Case C-403/08, Karen Murphy v Media Protection Services Ltd, Case C-429/08, (2012) EWHC 108.

Концепция злоупотребления авторским правом может еще больше прояснить рассматриваемую проблему. Хотя вопрос о возможном нарушении авторских прав в случае изобретений, созданных искусственным интеллектом, еще не до конца проработан, из прошлых решений судов ЕС по таким делам, как Deutsche Grammophon, Coditel I Coditel II и Metronome Musik[57], можно сделать некоторые выводы в отношении автора-человека и его действий в качестве правообладателя. Основополагающим понятием во всех вышеупомянутых делах является разумность, соразмерность и уместность «защиты моральных и экономических прав» автора[58]. При наличии автора-человека разумность, соразмерность и уместность приобретают форму разумного вознаграждения за коммерческое использование произведения. Когда автор-человек отсутствует, те же самые понятия должны принимать форму неприменения норм интеллектуальной собственности из-за отсутствия основной предпосылки защиты авторских прав. Когда какое-либо вмешательство человека присутствует, необходимо доказать, что оно является творческим, выходящим за рамки результатов работы искусственного интеллекта. Согласно законодательству Европейского союза об авторском праве, требуется «...'обязательное' участие оператора (без этого участия произведение не было бы создано)» (Xalabarder, 2016). В отношении произведения, созданного с использованием искусственного интеллекта, вопрос должен заключаться в следующем: является ли вклад человека необходимым для его материализации?

Исходя из этого, необходима нормативная база, которая предоставит нам пошаговые рекомендации. Так же, как был принят Закон ЕС об ИИ, можно разработать и внедрить закон об ИИ и интеллектуальной собственности. Прежде чем приступить к такому развитию права, нужно представить, что может привести к его появлению.

Первоначальным предварительным условием могло бы стать обязательное ведение патентными органами журналов регистрации, фиксирующих каждый шаг до момента создания окончательной версии произведения и вклад каждого «действующего лица» – как человека, так и искусственного интеллекта – в конечный результат. Это обязательное условие для того, чтобы можно было в дальнейшем качественно и количественно оценить вклад каждого участника. Эти журналы должны предоставляться соответствующим органам и должны быть доступны для оценки, чтобы человек мог претендовать на защиту авторских прав.

На основе этого первого шага вторым могла бы стать реконструкция творческого процесса. Необходимо определить некоторые критические пороговые значения креативности: выбор области интересов, т. е. в какой научной или промышленной области будут предприниматься попытки творчества; описание оригинальной идеи и ее более поздних версий; данные, на основе которых будет проводиться обучение; повторяющиеся действия, пока оригинальная идея или ее варианты не будут окончательно доработаны. Очевидно, что не все эти этапы имеют одинаковую качественную ценность для концепции и конечного результата творческой работы.

---

57 Case C-78/70 Deutsche Grammophon Gesellschaft mbH v. Metro-SB-Großma¨rkte GmbH & Co; KG.Deutsche Grammophon v. Metro SB [1971] ECR 487, para. 11; Case C-262/81 Coditel v. Cine´Vog Films II (Coditel II) [1982] ECR 3381; Case C-200/96, Metronome Musik GmbH v. Music Point Hokamp GmbH [1998] ECR I-1953; (Xalabarder, 2016).

58 Case 158/86 Warner Brothers and Another v. Christiansen [1988] ECR 2605, para. 13.

С помощью журналов регистрации соответствующие органы смогут определить, кто является субъектом причинно-следственной связи между концепцией и ее промышленным применением. Для того чтобы произведение соответствовало требованиям авторского права, должно быть доказано, что именно человеческий интеллект стоит как за концепцией идеи, так и за той работой, которая необходима для того, чтобы эта идея нашла промышленное применение. Если человек не в состоянии доказать и концепцию идеи, и ее преобразование в промышленное применение, то о защите авторских прав не может быть и речи. Второстепенного вклада человека, такого как улучшения в окончательной работе или ее частичный пересмотр, будет недостаточно для защиты авторских прав. Очевидно, что административные и судебные органы должны будут провести соответствующую оценку.

Конечно, могут возникнуть ситуации, когда независимо от предоставления каких-либо журналов регистрации будет невозможно определить, является ли человек или искусственный интеллект объектом причинно-следственной связи, из-за постоянного взаимодействия между ними. В таком случае, при тесном и в равной степени творческом сотрудничестве между человеком и искусственным интеллектом, опять же было бы несправедливо, если бы человек получал прибыль, поскольку он не является единственным создателем произведения. Даже если сроки защиты авторских прав будут сокращены, в течение этого периода человек получит выгоду от того, что не является продуктом исключительно его работы. Таким образом, запрос должен касаться исключительно авторства человека, а бремя доказывания должно лежать на человеке.

Заключение

Законодательство ЕС сталкивается с растущими проблемами, связанными с влиянием новых технологий, и особенно искусственного интеллекта, на нормы интеллектуальной собственности (Rosati, 2014). На самом деле с такими трудностями сталкивается не только правовая система ЕС, но и правовые системы во всем мире. Искусственный интеллект ставит новые задачи как перед законодателями, так и перед судами, которые, особенно в соответствии с законодательством ЕС, сыграли значительную роль в формировании норм в области интеллектуальной собственности (Favale et al., 2016). Не подлежит сомнению, что искусственный интеллект беспрецедентно преобразует сферу интеллектуальной собственности (Cabay & Lambrecht, 2015).

Нормы в области интеллектуальной собственности не являются абсолютными. Они должны быть сбалансированы с общественными интересами и конкурентными правами. Такие положения содержатся в национальных законодательствах ряда государств – членов ЕС, а также в законодательстве ЕС. Хотя точная степень защиты интеллектуальной собственности как на конституционном уровне, так и на уровне обычных законов в разных государствах-членах различается, необходимость сбалансированного подхода не ставится под сомнение[59]. Европейский суд по правам человека также придерживается этой позиции. В делах Scarlet Extended и NetLog суд постановил, что, хотя права интеллектуальной собственности защищены, «ничто

[59] Geller, P. E. (2009–2010). A German Approach to Fair Use. Test Cases for TRIPS Criteria for Copyright Limitations, in 57 Journal of the Copyright Society of the USA 553, 907; Moscarini, A. (2006). Proprietà privata e tradizioni costituzionali comuni, Milano, 2006, 161 ff.

в формулировке этого положения или в прецедентной практике Суда не указывает на то, что это право является нерушимым и по этой причине должно быть абсолютно защищено»[60]. Защита интеллектуальной собственности должна быть справедливой по отношению к автору (поощрять личные достижения) и пропорциональной общественным интересам, которые требуют максимально широкого доступа к знаниям, творениям и их промышленному применению.

Идея этой статьи заключается в том, что ИИ, создавая произведения, может быть онтологически творческим, несмотря на то, что его изобретения не могут быть защищены законом об авторском праве. ИИ – это не просто автомат, это уникальный, самостоятельный субъект, обладающий способностью к автономному творчеству. Таким образом, запрет публичного доступа к его произведениям является несправедливым, непропорциональным и оскорбительным с точки зрения норм интеллектуальной собственности как в соответствии с законодательством ЕС, так и в соответствии с международным законодательством об авторском праве. На самом деле нам необходим новый набор норм и предписаний в соответствии с законодательством ЕС, своего рода стандарты и показатели автономии ИИ, которые помогут определить, когда ИИ становится настолько автономным, что его результаты должны быть свободно доступны всем нам. Фундаментальным требованием должна быть всеобщая доступность произведений, созданных с использованием ИИ. Это должно стать новым руководящим принципом в наступающую эпоху произведений, созданных с помощью ИИ.

Список литературы

Adler, A. (2009.). Against moral rights. *California Law Review*, *97*, 263–301.

Bently, L., & Sherman, B. (2014). *Intellectual property law*. New York: Oxford University Press.

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.

Bostrom, N., & Ćirkovic, M. (2008). Introduction. In N. Bostrom, M., Ćirkovic, & M. Rees (Eds.), *Global Catastrophic Risks*. Oxford: Oxford University Press.

Butler, T. L. (1982). Can a computer be an author – copyright aspects of artificial intelligence. *Hastings Communications and Entertainment Law Journal*, *4*, 707.

Cabay, J., & Lambrecht, M. (2015). Remix prohibited: how rigid EU copyright laws inhibit creativity. *Journal of Intellectual Property Law & Practice*, *10*(5), 359–377. https://doi.org/10.1093/jiplp/jpv015

Castelvecchi, D. (2016). Can we open the black box of AI? *Nature*, *538*(7623), 22. https://doi.org/10.1038/538020a

Cohen, Ju. E. (2006). Copyright, Commodification, and Culture: Locating the Public Domain. In L. Guibault, & P. B. Hugenholtz (Eds.), *The Future of the Public Domain* (pp. 121–166). Kluwer Law Intl.

Favale, M., Kretschmer, M., & Torremans, P. C. (2016). Is there an EU Copyright Jurisprudence? An Empirical Analysis of the Workings of the European Court of Justice. *The Modern Law Review*, *79*, 31–75. https://doi.org/10.1111/1468-2230.12166

Fisher, W. W. (2001). Theories of Intellectual Property. In S. Munzer (Ed.), *New Essays in the Legal and Political Theory of Property* (pp. 168–199). Cambridge University Press.

Gerdes, A. (2018). An Inclusive Ethical Design Perspective for a Flourishing Future with Artificial Intelligent Systems. *European Journal of Risk Regulation*, *9*(4), 677–689. https://doi.org/10.1017/err.2018.62

Gervais, D. J. (2019). The machine as author. *Iowa Law Review*, *105*, 2053–2106.

Ginsburg, J. C. (2018). People Not Machines: Authorship and What It Means in the Berne Convention. *International Review of Intellectual Property and Competition Law (IIC)*, *49*, 131. https://doi.org/10.1007/S40319-018-0670-X

Ginsburg, J. C., & Budiardjo, L. A. (2019). Authors and machines. *Berkeley Technology Law Journal*, *34*(2), 343. https://doi.org/10.2139/ssrn.3233885

[60] Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10, 24 November 2011, para. 43.

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

Grinmelmann, J. (2016). There's No Such Thing as a Computer-Authored Work – and It's a Good Thing, Too. *Columbia Journal of Law & the Arts*, *39*, 403. https://doi.org/10.31228/osf.io/rk8cm

Hallevy, G. (2018). *Dangerous Robots – Artificial Intelligence vs. Human Intelligence*. http://dx.doi.org/10.2139/ssrn.3121905

Hansmann, H., & Santilli, M. (1997). Authors' and artists' moral rights: a comparative legal and economic analysis. *The Journal of Legal Studies*, *26*(1), 95. https://doi.org/10.1086/467990

Hashiguchi, M. (2017a). The global artificial intelligence revolution challenges patent eligibility laws. *Journal of Business & Technology Law*, *13*(1).

Hashiguchi, M. (2017b). Artificial intelligence and the jurisprudence of patent eligibility in the United States, Europe, and Japan. *Intellectual Property & Technology Law Journal*, *29*(12), 3–15.

Hattenbach, B., & Snyder, G. (2018). Rethinking the mental steps doctrine and other barriers to patentability of artificial intelligence. *Columbia Science and Technology Law Review*, *19*(2), 313–339.

Hemel, D. J., & Ouellette, L. L. (2013). Beyond the Patents–Prizes Debate. *Texas Law Review*, *92*(2), 303. https://doi.org/10.2139/ssrn.2245691

Holst, K. (2006.). A case of bad credit?: The United States and the protection of moral rights in intellectual property law. *Buffalo Intellectual Property Law Journal*, *3*(2), 105.

Hristov, K. (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA*, *57*, 431.

Hugenholtz, P. B., & Quintais, J. P. (2021). Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output? (2021). *International Review of Intellectual Property and Competition Law – IIC*, 52, 1190–1216. https://doi.org/10.1007/s40319-021-01115-0

Hutter, M. (2010). *Universal Artificial Intelligence: Sequential Decisions Based on Algorithmic Probability*. Springer.

Hutukka, P. (2023). Copyright Law in the European Union, the United States and China. *International Review of Intellectual Property and Competition Law – IIC*, 54, 1044–1080. https://doi.org/10.1007/s40319-023-01357-0

Jaszi, P. (1992). On the Author Effect: Contemporary Copyright and Collective Creativity. *Cardozo Arts & Entertainment Law Journal*, *10*(2), 293–320.

Karppi, T., & Crawford, K. (2016). Social Media, Financial Algorithms and the Hack Crash. *Theory Culture & Society*, *33*(1), 73. https://doi.org/10.1177/0263276415583139

Khoury, A. H. (2017). Intellectual Property Rights For "Hubots": On The Legal Implications Of Human-Like Robots As Innovators And Creators. *Cardozo Arts & Entertainment Law Journal*, *35*(3), 635–668.

Krauss, M. (1989). Property, Monopoly, and Intellectual Rights Non-Posnerian Law and Economics Symposium. *Hamline Law Review*, *12*(2), 305.

Kur, A., Dreier, T., & Luginbuehl, S. (2013). *European intellectual property law: text, cases and materials* (2nd edn.). Edward Elgar Publishing, Cheltenham.

Lake, B. Ullman, T., Tenenbaum, J., & Gershman, S. (2017). Building Machines That Learn and Think Like People. *Behavioral and brain sciences*, *40*, 1–72. https://doi.org/10.1017/S0140525X16001837

Laton, D. (2016). Manhattan_Project.Exe: A Nuclear Option for the Digital Age. *Catholic University Journal of Law & Technology*, *25*(1), 94.

Manderieux, L. (2010). Secured Transactions as a Tool for Better Use of Intellectual Property Rights and of Intellectual Property Licensing (including Patent Licensing). *UNIDROIT Uniform Law Review*, *2010-1*, 447.

Martinez, R. (2019). Artificial Intelligence: Distinguishing Between Types & Definitions. *Nevada Law Journal*, *19*(3), 1015–1041.

McCarthy, J. (2008). The Well-Designed Child. *Artificial Intelligence*, *172*(18). https://doi.org/10.1016/j.artint.2008.10.001

Mizaras, V. (2012). Lithuania, In R. M. Hilty, & S, Ne´risson (Eds), *Balancing copyright – a survey of national approaches* (pp. 623–644). Springer, Berlin.

Omohundro, S. M. (2008). The Basic AI Drives. In Pei Wang et al. (Eds.), *Artificial General Intelligence 2008: Proceedings Of The First Agi Conference* (p. 483).

Pila, J., & Torremans, P. (2019). *European Intellectual Property Law*. Oxford University Press.

Rai, Arti Kaur. (1999). Regulating Scientific Research: Intellectual Property Rights and the Norms of Science. *Northwestern University Law Review*, *94*, 77. https://doi.org/10.2139/ssrn.172032

Ricketson, S., & Ginsburg, J. (2005). *International copyright and neighbouring rights: The Berne Convention and beyond* (2d ed.). New York: Oxford University Press.

Rosati, E. (2014). Copyright in the EU: in search of (in)flexibilities. *Journal of Intellectual Property Law & Practice*, *9*(7), 585–598. https://doi.org/10.1093/jiplp/jpu034

Russell, S. J., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3d ed.). Pearson.
Salzberger, E. (2006). Economic Analysis of the Public Domain In L. Guibault, & P. B. Hugenholtz (Eds.), *The Future of the Public Domain* (Ch. III, pp. 27–59). Kluwer Law Intl.
Senftleben, M., & Buijtelaar, L. (2020). Robot creativity: an incentive-based neighboring rights approach. *European Intellectual Property Review*, *42*, 797–806. https://doi.org/10.2139/ssrn.3707741
Sganga, C., & Scalzini, S. (2017). From Abuse of Right to European Copyright Misuse: A New Doctrine for EU Copyright Law. *International Review of Intellectual Property and Competition Law (IIC)*, *48*(4), 405–435. https://doi.org/10.1007/s40319-017-0584-z
Sobel, B. L. W. (2017). Artificial Intelligence's Fair Use Crisis. *Columbia Journal of Law & The Arts*, *41*(1), 45–97. https://doi.org/10.7916/jla.v41i1.2036
Spector, L. (2006). Evolution of artificial intelligence. *Artificial Intelligence*, *170*(18), 1251–1253. https://doi.org/10.1016/j.artint.2006.10.009
Suchman, L., & Weber, J. (2016). Human-Machine Autonomies. In N. Bhuta, S. Beck, R. Geib, H. Yan Liu, & C. Kreb (Eds.), *Autonomous Weapon Systems: Law, Ethics, Policy* (pp. 39, 40). Cambridge: Cambridge University Press.
Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, *49*(236), 433–460. https://doi.org/10.1093/mind/lix.236.433
Van Asselt, M. B. A., & Renn, O. (2011). Risk Governance. *Journal of Risk Research*, *14*(4), 431–449. https://doi.org/10.1080/13669877.2011.553730
van Eechoud, M. (2012). Along the road to uniformity: diverse readings of the Court of Justice Judgments on copyright works. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *3*(1), 60–80.
van Gompel, S. (2014). Creativity, autonomy and personal touch. A critical appraisal of the CJEU's originality test for copyright. In M. van Eechoud (Ed.), *The work of authorship* (pp. 95–143). Amsterdam: University Press.
Walter, M., & von Lewinski, S. (2010). *European copyright law: a commentary*. New York: Oxford University Press.
Xalabarder, R. (2016). The Role of the CJEU in Harmonizing EU Copyright Law. *International Review of Intellectual Property and Competition Law – IIC*, *47*, 635–639. https://doi.org/10.1007/s40319-016-0509-2
Xu, M, David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research*, *9*(2), 90–95. https://doi.org/10.5430/ijfr.v9n2p90
Yanisky-Ravid, S., & Liu, X. (2018). When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law. *Cardozo Law Review*, *39*, 2215–2263.
Yong, Wan, & Hongxuyang, Lu. (2021). Copyright protection for AI-generated outputs: The experience from China. *Computer Law & Security Review*, *42*. https://doi.org/10.1016/j.clsr.2021.105581
Zurth, P. (2021). Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law & Technology*, *25*(2).

Сведения об авторе

Цимас Фемистоклис – PhD в области государственного международного права и политологии, ассистент преподавателя, Школа права, Университет Фракии имени Демокрита
Адрес: Греция, PS 66100, г. Комотини, Университетский кампус
E-mail: themis.tzimas@gmail.com
ORCID ID: https://orcid.org/0000-0002-0454-8220
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56615756300
Google Scholar ID: https://scholar.google.com/citations?user=XYVSDaIAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.41.51 / Охрана авторских прав
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 20 октября 2024 г.
Дата одобрения после рецензирования – 8 ноября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:347.78:340.13:347.9:004.8
EDN: https://elibrary.ru/ppfjub
DOI: https://doi.org/10.21202/jdtl.2025.2

Evolution of Copyright in the Era of Artificial Intelligence: Analysis of Conflicts of Law and Judicial Precedents

Themistoklis Tzimas

Democritus University of Thrace, Komotini, Greece

Keywords

artificial intelligence,
copyright law,
court,
digital technologies,
intellectual property,
interdisciplinary approach,
law,
legal regulation,
legislation,
technological advancement

Abstract

Objective: a comprehensive critical analysis of the modern legal regulation of artificial intelligence technologies arising at the junction of intellectual property and artificial intelligence norms. Special attention is paid to the study of conflicts between existing European copyright legislation and new technological realities.

Methods: the work uses an interdisciplinary approach, including historical, formal-legal and comparative-legal research methods. The historical method allowed tracing the evolution of legislative and doctrinal approaches to intellectual property regulation in the era of digitalization. The formal-legal method made it possible to conduct a detailed analysis of the legal norms of various states. The comparative-legal method provided an opportunity to compare different approaches to regulating relations in the use of artificial intelligence for creative activities.

Results: the study examines the issues of copyright for works created using artificial intelligence, including complex aspects of determining authorship, as well as the issues of anthropocentrism in modern legislation. The author analyzes judicial precedents, mainly in the context of the European Union legislation, which is actively adapting to new technological challenges. Various approaches are investigated to determine the legal status of works created using artificial intelligence and their impact on traditional intellectual property concepts.

Scientific novelty: the article presents a unique comprehensive assessment of the impact of the AI creative capabilities on the fundamental intellectual

property concepts. The scientific significance lies in the author's original assessment of the impact of artificial intelligence technologies on copyright legislation, based on a detailed analysis of judicial precedents and doctrinal approaches. The author investigate the prospective development of legal regulation in the context of technological progress.

Practical significance: the paper proposes legal and governmental solutions aimed at creating a balanced and effective intellectual property regime in the era of artificial intelligence. Recommendations were developed to improve legislation, taking into account existing judicial precedents and the needs of the digital economy. The research results can be used to develop new regulations and improve the existing legal framework of artificial intelligence regulation.

For citation

Tzimas, Th. (2025). Evolution of Copyright in the Era of Artificial Intelligence: Analysis of Conflicts of Law and Judicial Precedents. *Journal of Digital Technologies and Law, 3*(1), 35–64. https://doi.org/10.21202/jdtl.2025.2

References

Adler, A. (2009.). Against moral rights. *California Law Review*, *97*, 263–301.

Bently, L., & Sherman, B. (2014). *Intellectual property law*. New York: Oxford University Press.

Bostrom, N. (2014). *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press.

Bostrom, N., & Ćirkovic, M. (2008). Introduction. In N. Bostrom, M., Ćirkovic, & M. Rees (Eds.), *Global Catastrophic Risks*. Oxford: Oxford University Press.

Butler, T. L. (1982). Can a computer be an author – copyright aspects of artificial intelligence. *Hastings Communications and Entertainment Law Journal*, *4*, 707.

Cabay, J., & Lambrecht, M. (2015). Remix prohibited: how rigid EU copyright laws inhibit creativity. *Journal of Intellectual Property Law & Practice*, *10*(5), 359–377. https://doi.org/10.1093/jiplp/jpv015

Castelvecchi, D. (2016). Can we open the black box of AI? *Nature*, *538*(7623), 22. https://doi.org/10.1038/538020a

Cohen, Ju. E. (2006). Copyright, Commodification, and Culture: Locating the Public Domain. In L. Guibault, & P. B. Hugenholtz (Eds.), *The Future of the Public Domain* (pp. 121–166). Kluwer Law Intl.

Favale, M., Kretschmer, M., & Torremans, P. C. (2016). Is there an EU Copyright Jurisprudence? An Empirical Analysis of the Workings of the European Court of Justice. *The Modern Law Review*, *79*, 31–75. https://doi.org/10.1111/1468-2230.12166

Fisher, W. W. (2001). Theories of Intellectual Property. In S. Munzer (Ed.), *New Essays in the Legal and Political Theory of Property* (pp. 168–199). Cambridge University Press.

Gerdes, A. (2018). An Inclusive Ethical Design Perspective for a Flourishing Future with Artificial Intelligent Systems. *European Journal of Risk Regulation*, *9*(4), 677–689. https://doi.org/10.1017/err.2018.62

Gervais, D. J. (2019). The machine as author. *Iowa Law Review*, *105*, 2053–2106.

Ginsburg, J. C. (2018). People Not Machines: Authorship and What It Means in the Berne Convention. *International Review of Intellectual Property and Competition Law (IIC)*, *49*, 131. https://doi.org/10.1007/S40319-018-0670-X

Ginsburg, J. C., & Budiardjo, L. A. (2019). Authors and machines. *Berkeley Technology Law Journal*, *34*(2), 343. https://doi.org/10.2139/ssrn.3233885

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

Grinmelmann, J. (2016). There's No Such Thing as a Computer-Authored Work – and It's a Good Thing, Too. *Columbia Journal of Law & the Arts*, *39*, 403. https://doi.org/10.31228/osf.io/rk8cm

Hallevy, G. (2018). *Dangerous Robots – Artificial Intelligence vs. Human Intelligence*. http://dx.doi.org/10.2139/ssrn.3121905

Hansmann, H., & Santilli, M. (1997). Authors' and artists' moral rights: a comparative legal and economic analysis. *The Journal of Legal Studies*, *26*(1), 95. https://doi.org/10.1086/467990

Hashiguchi, M. (2017a). The global artificial intelligence revolution challenges patent eligibility laws. *Journal of Business & Technology Law*, *13*(1).

Hashiguchi, M. (2017b). Artificial intelligence and the jurisprudence of patent eligibility in the United States, Europe, and Japan. *Intellectual Property & Technology Law Journal*, *29*(12), 3–15.

Hattenbach, B., & Snyder, G. (2018). Rethinking the mental steps doctrine and other barriers to patentability of artificial intelligence. *Columbia Science and Technology Law Review*, *19*(2), 313–339.

Hemel, D. J., & Ouellette, L. L. (2013). Beyond the Patents–Prizes Debate. *Texas Law Review*, *92*(2), 303. https://doi.org/10.2139/ssrn.2245691

Holst, K. (2006.). A case of bad credit?: The United States and the protection of moral rights in intellectual property law. *Buffalo Intellectual Property Law Journal*, *3*(2), 105.

Hristov, K. (2017). Artificial Intelligence and the Copyright Dilemma. *IDEA*, *57*, 431.

Hugenholtz, P. B., & Quintais, J. P. (2021). Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output? (2021). *International Review of Intellectual Property and Competition Law – IIC*, 52, 1190–1216. https://doi.org/10.1007/s40319-021-01115-0

Hutter, M. (2010). *Universal Artificial Intelligence: Sequential Decisions Based on Algorithmic Probability*. Springer.

Hutukka, P. (2023). Copyright Law in the European Union, the United States and China. *International Review of Intellectual Property and Competition Law – IIC*, 54, 1044–1080. https://doi.org/10.1007/s40319-023-01357-0

Jaszi, P. (1992). On the Author Effect: Contemporary Copyright and Collective Creativity. *Cardozo Arts & Entertainment Law Journal*, *10*(2), 293–320.

Karppi, T., & Crawford, K. (2016). Social Media, Financial Algorithms and the Hack Crash. *Theory Culture & Society*, *33*(1), 73. https://doi.org/10.1177/0263276415583139

Khoury, A. H. (2017). Intellectual Property Rights For "Hubots": On The Legal Implications Of Human-Like Robots As Innovators And Creators. *Cardozo Arts & Entertainment Law Journal*, *35*(3), 635–668.

Krauss, M. (1989). Property, Monopoly, and Intellectual Rights Non-Posnerian Law and Economics Symposium. *Hamline Law Review*, *12*(2), 305.

Kur, A., Dreier, T., & Luginbuehl, S. (2013). *European intellectual property law: text, cases and materials* (2nd edn.). Edward Elgar Publishing, Cheltenham.

Lake, B. Ullman, T., Tenenbaum, J., & Gershman, S. (2017). Building Machines That Learn and Think Like People. *Behavioral and brain sciences*, *40*, 1–72. https://doi.org/10.1017/S0140525X16001837

Laton, D. (2016). Manhattan_Project.Exe: A Nuclear Option for the Digital Age. *Catholic University Journal of Law & Technology*, *25*(1), 94.

Manderieux, L. (2010). Secured Transactions as a Tool for Better Use of Intellectual Property Rights and of Intellectual Property Licensing (including Patent Licensing). *UNIDROIT Uniform Law Review*, *2010-1*, 447.

Martinez, R. (2019). Artificial Intelligence: Distinguishing Between Types & Definitions. *Nevada Law Journal*, *19*(3), 1015–1041.

McCarthy, J. (2008). The Well-Designed Child. *Artificial Intelligence*, *172*(18). https://doi.org/10.1016/j.artint.2008.10.001

Mizaras, V. (2012). Lithuania, In R. M. Hilty, & S, Ne´risson (Eds), *Balancing copyright – a survey of national approaches* (pp. 623–644). Springer, Berlin.

Omohundro, S. M. (2008). The Basic AI Drives. In Pei Wang et al. (Eds.), *Artificial General Intelligence 2008: Proceedings Of The First Agi Conference* (p. 483).

Pila, J., & Torremans, P. (2019). *European Intellectual Property Law*. Oxford University Press.

Rai, Arti Kaur. (1999). Regulating Scientific Research: Intellectual Property Rights and the Norms of Science. *Northwestern University Law Review*, *94*, 77. https://doi.org/10.2139/ssrn.172032

Ricketson, S., & Ginsburg, J. (2005). *International copyright and neighbouring rights: The Berne Convention and beyond* (2d ed.). New York: Oxford University Press.

Rosati, E. (2014). Copyright in the EU: in search of (in)flexibilities. *Journal of Intellectual Property Law & Practice*, *9*(7), 585–598. https://doi.org/10.1093/jiplp/jpu034

Russell, S. J., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach* (3d ed.). Pearson.

Salzberger, E. (2006). Economic Analysis of the Public Domain In L. Guibault, & P. B. Hugenholtz (Eds.), *The Future of the Public Domain* (Ch. III, pp. 27–59). Kluwer Law Intl.

Senftleben, M., & Buijtelaar, L. (2020). Robot creativity: an incentive-based neighboring rights approach. *European Intellectual Property Review*, *42*, 797–806. https://doi.org/10.2139/ssrn.3707741

Sganga, C., & Scalzini, S. (2017). From Abuse of Right to European Copyright Misuse: A New Doctrine for EU Copyright Law. *International Review of Intellectual Property and Competition Law (IIC)*, *48*(4), 405–435. https://doi.org/10.1007/s40319-017-0584-z

Sobel, B. L. W. (2017). Artificial Intelligence's Fair Use Crisis. *Columbia Journal of Law & The Arts*, *41*(1), 45–97. https://doi.org/10.7916/jla.v41i1.2036

Spector, L. (2006). Evolution of artificial intelligence. *Artificial Intelligence*, *170*(18), 1251–1253. https://doi.org/10.1016/j.artint.2006.10.009

Suchman, L., & Weber, J. (2016). Human-Machine Autonomies. In N. Bhuta, S. Beck, R. Geib, H. Yan Liu, & C. Kreb (Eds.), *Autonomous Weapon Systems: Law, Ethics, Policy* (pp. 39, 40). Cambridge: Cambridge University Press.

Turing, A. M. (1950). Computing Machinery and Intelligence. *Mind*, *49*(236), 433–460. https://doi.org/10.1093/mind/lix.236.433

Van Asselt, M. B. A., & Renn, O. (2011). Risk Governance. *Journal of Risk Research*, *14*(4), 431–449. https://doi.org/10.1080/13669877.2011.553730

van Eechoud, M. (2012). Along the road to uniformity: diverse readings of the Court of Justice Judgments on copyright works. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, *3*(1), 60–80.

van Gompel, S. (2014). Creativity, autonomy and personal touch. A critical appraisal of the CJEU's originality test for copyright. In M. van Eechoud (Ed.), *The work of authorship* (pp. 95–143). Amsterdam: University Press.

Walter, M., & von Lewinski, S. (2010). *European copyright law: a commentary*. New York: Oxford University Press.

Xalabarder, R. (2016). The Role of the CJEU in Harmonizing EU Copyright Law. *International Review of Intellectual Property and Competition Law – IIC*, *47*, 635–639. https://doi.org/10.1007/s40319-016-0509-2

Xu, M, David, J. M., & Kim, S. H. (2018). The Fourth Industrial Revolution: Opportunities and Challenges. *International Journal of Financial Research*, *9*(2), 90–95. https://doi.org/10.5430/ijfr.v9n2p90

Yanisky-Ravid, S., & Liu, X. (2018). When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law. *Cardozo Law Review*, *39*, 2215–2263.

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

Zurth, P. (2021). Artificial Creativity? A Case against Copyright Protection for AI-Generated Works. *UCLA Journal of Law & Technology*, *25*(2).

Author information

Themistoklis Tzimas – PhD (Public International Law and Political Science), Adjunct Assistant Professor, School of Law, Democritus University of Thrace
Address: PS 66100, University Campus, Komotini, Greece
E-mail: themis.tzimas@gmail.com
ORCID ID: https://orcid.org/0000-0002-0454-8220
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=56615756300
Google Scholar ID: https://scholar.google.com/citations?user=XYVSDaIAAAAJ

Conflict of interest

The author declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

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

Article history

Date of receipt – October 20, 2024
Date of approval – November 8, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:343.3/.7:004.056:004.9
EDN: https://elibrary.ru/rtolza
DOI: https://doi.org/10.21202/jdtl.2025.3

Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру

Нилкант Бхатт

Инженерный колледж Лухдхирджи, Морби, Индия

Ключевые слова

безопасность,
искусственный интеллект,
качество продукции,
метод PESTEL,
право,
преступление,
преступность,
уголовная ответственность,
уголовное законодательство,
цифровые технологии

Аннотация

Цель: изучение применимости существующих норм об ответственности за качество продукции и законов о халатности к преступлениям, связанным с использованием искусственного интеллекта. Автор выдвигает гипотезу о том, что гибридное применение этих правовых механизмов может стать основой для создания эффективной системы регулирования в условиях стремительного развития технологий.

Методы: комплексный подход, основанный на анализе PESTEL (политические, экономические, социальные, технологические, экологические и правовые факторы), методе анализа первопричин «Пять почему» и изучении кейсов из различных стран. Такой многоуровневый подход позволяет не только выявить ключевые проблемы, но и предложить адаптированные решения, учитывающие специфику преступлений, связанных с искусственным интеллектом.

Результаты: исследование демонстрирует, что существующие нормы об ответственности за качество продукции и халатности недостаточно эффективны для регулирования преступлений, связанных с искусственным интеллектом. Основными препятствиями являются технологическая сложность, отсутствие прецедентов, недостаточная осведомленность потребителей и юрисдикционные проблемы. Автор приходит к выводу, что для эффективного регулирования необходима глобальная система, включающая четкие принципы ответственности, строгие стандарты безопасности и постоянную адаптацию к новым вызовам.

Научная новизна: заключается в уникальном подходе к изучению преступлений, связанных с искусственным интеллектом, через призму гибридного применения существующих правовых механизмов. Исследование предлагает новый взгляд на проблему, сочетая теоретический анализ с практическими рекомендациями, основанными на изучении реальных кейсов.

Практическая значимость: состоит в разработке конкретных рекомендаций для законодателей и регулирующих органов. Автор подчеркивает необходимость создания специализированных органов, внедрения образовательных программ для граждан и сотрудников, а также обеспечения финансирования исследований в области объяснимого искусственного интеллекта и стандартов безопасности. Эти меры направлены на формирование устойчивой системы регулирования, способной эффективно противостоять преступлениям, связанным с использованием искусственного интеллекта. Работа открывает новые горизонты для дальнейших исследований в области регулирования технологий искусственного интеллекта, подчеркивая необходимость международного сотрудничества и междисциплинарного подхода.

Для цитирования

Бхатт, Н. (2025). Преступления в эпоху искусственного интеллекта: гибридный подход к ответственности и безопасности в цифровую эру. *Journal of Digital Technologies and Law*, *3*(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

Содержание

Введение

Термин «преступления, совершенные с использованием искусственного интеллекта (ИИ)» появился недавно, но уже стал хорошо известен. Он обозначает преступления, в которых искусственный интеллект (далее – ИИ) используется как инструмент для создания подделок с целью мошенничества, обмана и манипуляций[1]. Технологии ИИ

[1] Center for AI Crime. (2023). About AI Crimes. https://clck.ru/3Gpr34

также могут использоваться преступниками для обхода систем безопасности или манипулирования процессом принятия решений (King et al., 2021). Растущие возможности ИИ позволяют совершать беспрецедентные по масштабу преступления, а также усложнять задачу принятия необходимых мер защиты[2].

По мере того как ИИ набирает силу, растет и потенциал его преступного использования. Это может привести к появлению новых видов преступной деятельности и к увеличению числа жертв преступности. Существуют ли средства борьбы с этими явлениями? Поспешное изменение регулирования может привести к тому, что оно быстро устареет.

Применимость существующих законов к новым видам преступлений с использованием ИИ – это сложная проблема. Утверждается, что действующие правовые рамки универсальны и могут быть адаптированы к новым видам преступлений; например, к дипфейкам, используемым в финансовой сфере, могут применяться уголовные законы о мошенничестве. Однако другие авторы обращают внимание на ограниченность существующих правовых норм в борьбе с подобными преступлениями. Так, в работе Sukhodolov и др. (2020) отмечается, что существующие законы недостаточно адекватно учитывают такие аспекты преступлений с использованием ИИ, как преступный умысел, так как преступления с умыслом обычно совершаются людьми. Непрозрачность алгоритмов искусственного интеллекта не позволяет решить вопрос об ответственности за преступление (Sukhodolov et al., 2020).

Отсутствие ясности в отношении подсудности и ответственности, неадекватность правового режима, трудности с определением вины и юрисдикционные проблемы – вот некоторые основные причины, по которым существующее уголовное законодательство оказывается недостаточным для рассмотрения дел, связанных с преступлениями с использованием ИИ. Кроме того, применение уголовного законодательства в отношении преступлений, связанных с технологиями или продуктами искусственного интеллекта, требует установления элементов умысла и атрибуции. Необходимо неопровержимо доказать, что преступление с использованием ИИ было совершено с умыслом и что оно связано с субъектом, совершившим его. Однако технологии могут причинять вред непреднамеренно. Также довольно сложно доказать, что преступление совершено программистом, производителем или пользователем ИИ. Это мешает задачам судебного преследования и эффективного сдерживания преступности. Поэтому необходимо создавать более надежную правовую базу в сфере постоянно развивающихся технологий искусственного интеллекта.

В отличие от уголовного законодательства гражданское в первую очередь рассматривает обязанности и элемент предсказуемости, поэтому его легче применить к преступлениям с использованием ИИ. В этом случае речь идет о компенсации жертвам преступлений, а не о тюремном заключении или ином наказании преступников. Учитывая природу преступлений с использованием ИИ, жертвы должны получить предусмотренную компенсацию, но это не гарантирует предотвращения преступлений в будущем. Однако вред, причиняемый искусственным интеллектом, не всегда достигает уровня тяжких преступлений. В принципе, существующие традиционные законы, например, Закон об ответственности за качество продукции или Закон

[2] Markoff, J. (2016, October 23). As Artificial Intelligence Evolves, So Does Its Criminal Potential. The New York Times. https://clck.ru/3Gpr5Z

о халатности, вполне способны справиться с преступлениями с использованием ИИ, поскольку они направлены на обеспечение баланса между общественной безопасностью, ответственностью и развитием. Но в какой степени это является предметом рассмотрения?

В случае обнаружения дефектов продукции права клиента защищены законами об ответственности за качество продукции, поскольку производители, дистрибьюторы и продавцы несут за это ответственность. Аналогичным образом, если система искусственного интеллекта выходит из строя или причиняет ущерб, разработчик или производитель может быть привлечен к ответственности за такие дефекты (Scherer, 2015). С другой стороны, законы о халатности требуют от отдельных лиц проявлять должную осмотрительность при осуществлении действий по предотвращению ущерба. Эти законы можно применять к преступлениям с использованием ИИ, когда отдельные лица не в состоянии предотвратить неправомерное использование систем искусственного интеллекта для преступной деятельности (Zhao, 2024). Системы искусственного интеллекта ставят перед нами такие проблемы, как самостоятельность при принятии решений, способность к обучению и неучастие человека в преступных действиях. Таким образом, насущной необходимостью является специальная правовая база для противодействия таким преступлениям. Необходимо установить четкие руководящие принципы для определения ответственности и юрисдикции в этой сфере.

В идеале для обеспечения благоприятной ситуации для всех заинтересованных сторон в сфере ИИ система регулирования ИИ должна основываться на доктрине PEEC, то есть на идеях соблюдения «общественных интересов» и «принципов экологической устойчивости», «экономического развития» и «норм уголовного права» (Bhatt & Bhatt, 2023).

В настоящей работе выдвигается гипотеза о том, что «гибридное применение существующих Закона об ответственности за качество продукции (Product Liability Law, PLL) и Закона о халатности (Negligence Law, NL) обеспечивает надежную правовую основу в сфере преступлений, связанных с искусственным интеллектом». Цель исследования – подтвердить эту идею путем систематического рассмотрения и анализа конкретных примеров для изучения эффективности Закона об ответственности за качество продукции и Закона о халатности в сфере преступлений с использованием ИИ. Мы надеемся, что данное исследование станет началом научной дискуссии о совершенствовании регулирования искусственного интеллекта в развитом обществе.

1. Обзор литературы

Применимые условия существующего уголовного законодательства затрудняют регулирование преступлений, совершаемых с использованием ИИ (Qatawneh et al., 2023; Abbot & Sarch, 2019; Шестак и др., 2019). Применение традиционных принципов mens rea и actus reus также затруднено в случаях таких преступлений (Abbot & Sarch, 2019; Шестак и др., 2019). Во всем мире наблюдается устойчивый консенсус в отношении проведения законодательных реформ в сфере преступлений с использованием ИИ. Это относится и к уголовному законодательству (Qatawneh et al., 2023; Bhatt & Bhatt, 2023; Шестак и др., 2019; Khisamova & Begishev, 2019). Ряд экспертов предлагают внести незначительные изменения в существующие законы, в то время как другие считают, что изменения должны быть радикальными (Abbot & Sarch, 2019; Khisamova & Begishev, 2019). Для снижения возможных

рисков существует настоятельная потребность в стандартизации и сертификации при проектировании, разработке и внедрении технологий искусственного интеллекта (Khisamova & Begishev, 2019; Broadhurst et al., 2019). Высказывается также серьезная обеспокоенность по поводу потенциального нарушения искусственным интеллектом основных прав и закрепления предвзятости; ИИ может играть двоякую роль: способствовать совершению преступлений и предотвращать их (Broadhurst et al., 2019; Ivan & Manea, 2022). В работах Шестак с соавторами (2019) и Khan с соавторами (2021) обсуждаются модели ответственности за действия ИИ при определенных условиях, хотя автономность различных форм ИИ часто затрудняет применимость соответствующих законов. Несмотря на то, что системы искусственного интеллекта потенциально способствуют совершению преступлений, в будущем с ними может быть связана большая неопределенность (King et al., 2021). Существующая правовая база недостаточна для определения виновности в преступлениях, связанных с использованием искусственного интеллекта в качестве инструмента (Dremliuga & Prisekina, 2020). Технологии искусственного интеллекта могут соответствовать критериям уголовной ответственности, однако для решения этих проблем необходимы дополнительные усилия в области регулирования (Lagioia & Sartor, 2019).

Правовые нормы, нацеленные на решение проблем, связанных с ИИ, должны учитывать ряд жизненно важных принципов, включая установление однозначных руководящих критериев ответственности, внедрение строгих стандартов разработки и развертывания систем ИИ и формирование регулирующих органов для надзора и обеспечения соблюдения этих принципов. Кроме того, такая структура должна включать инструменты для постоянного мониторинга и обновлять их в соответствии с быстрым технологическим прогрессом, а также предусматривать международное сотрудничество с учетом глобального характера преступлений, связанных с ИИ (Binns, 2018; Calo, 2019; Gless, 2019). Предполагается, что система будет определять приоритетность защитных мер, включая обязательные аудиты безопасности и оценки этического воздействия разработки искусственного интеллекта (Jobin et al., 2019). Она должна адаптироваться к меняющемуся характеру систем ИИ, обеспечивая каналы для постоянного анализа и доработки.

Использование комплексного инструмента, сочетающего принципы ответственности за качество продукции с нормами законодательства о халатности, потенциально может решить важнейшие проблемы в сфере борьбы с преступлениями, связанными с ИИ. Законы об ответственности за качество продукции, в которых основное внимание уделяется конструктивным дефектам и стандартам безопасности (Solum, 2020), возлагают ответственность за недостатки систем искусственного интеллекта на их разработчиков. Согласно законодательству о халатности, которое постулирует обязанность проявлять добросовестность (Kingston, 2016), ответственность наступает за возможные риски, возникающие из-за неправильного развертывания или использования систем искусственного интеллекта. Этот гибридный подход обеспечивает комплексный инструмент для определения виновности и поощряет превентивные действия при разработке и использовании систем искусственного интеллекта.

В настоящее время как в развитых, так и в развивающихся странах существует ограниченная правовая база, касающаяся исключительно преступлений, связанных с ИИ. Европейский союз посредством Общего регламента по защите данных (General Data Protection Regulation, GDPR) и проекта закона об искусственном интеллекте предпринимает значительные шаги в решении проблем, связанных с технологиями

искусственного интеллекта[3, 4]. В Соединенных Штатах отсутствует всеобъемлющее регулирование, но различные ведомства используют свои руководящие принципы[5]. Сингапур предложил типовую систему регулирования искусственного интеллекта[6]. В 2021 г. Китай ввел несколько отраслевых нормативных актов в форме Руководящих положений по регулированию научно-технической деятельности в области искусственного интеллекта (Ли, 2023).

Российский подход направлен на развитие и поддержку, а не на ужесточение норм. В России разработана дорожная карта развития прорывных технологий «Нейротехнологии и искусственный интеллект» в рамках Национальной стратегии развития искусственного интеллекта на период до 2030 г.[7] В Индии также отсутствует единое регулирование, вместо этого четыре комитета отчитываются по различным аспектам ИИ и дают рекомендации по этичному развитию систем ИИ[8]. В Японии нет всеобъемлющих правовых норм, регулирующих технологию искусственного интеллекта, хотя Закон о защите личной информации от 2020 г. регулирует некоторые аспекты, связанные с системами искусственного интеллекта[9]. В Южной Корее также действует Рамочное положение по этике развития и использования искусственного интеллекта (2020), которые служат скорее руководящими принципами и не являются обязательными[10].

Проект по закону об ИИ, предложенный ЕС, предусматривает соблюдение строгих стандартов безопасности и четких норм ответственности в случае причинения вреда, подчеркивая важность управления рисками систем искусственного интеллекта. В США существует множество руководящих принципов в данной сфере, в которых основное внимание уделяется справедливости, подотчетности и снижению ущерба. Принципы действующих стандартов как в ЕС, так и в США соответствуют нормам законодательства об ответственности за качество продукции и о халатности.

2. Методология исследования

В настоящем исследовании используется рациональный, логичный, всеобъемлющий и многоуровневый подход к научному обоснованию выдвинутой гипотезы. Для отбора необходимой информации и правильного понимания внешних

3 European Commission. https://goo.su/y3Zuwv

4 Iapp.org (International Association of Privacy Professionals). Global AI Law and Policy Tracker. https://clck.ru/3Gpsti

5 National Institute of Standards and Technology (NIST). https://clck.ru/3GpszK

6 Singapore's AI Governance webpage. https://goo.su/uBEdf

7 Russia: Current status and development of AI regulations. (2024, May 24). Data Guidance. https://clck.ru/3GptAx

8 Government of India. (2018). Reports of various Committees on Artificial Intelligence. https://goo.su/H9dNS

9 Personal Information Protection Commission, Japan. https://clck.ru/3GptNq

10 Ministry of Science and ICT (MSIT), South Korea (2020). Framework for Ethical Development and Use of Artificial Intelligence. https://clck.ru/3GptTi

факторов, влияющих на гипотезу, был проведен анализ по методу PESTEL (political, economic, social, technological, environmental, legal), охватывающий политический, экономический, социальный, технологический, экологический и правовой аспекты с целью выявления факторов, которые находятся вне непосредственного контроля, но могут существенно повлиять на гипотезу. Наше исследование направлено не на устранение симптомов, а на решение реальных проблем путем глубокого и систематического разбора первопричины проблемы по методу «Пять почему».

Кроме того, для оценки различных мнений и расширения базы источников в работе использовались различные примеры для сравнения существующих законов об ответственности за качество продукции и о халатности в разных странах. Также мы рассмотрели успешные решения, эффективно внедренные в других областях. Этот комплексный анализ позволил выдвинуть предложения, направленные на устранение выявленной основной причины проблемы, а также адаптировать указанные решения к потенциальным последствиям их реализации.

Этот многогранный надежный подход не только основан на широком контексте, но и хорошо подходит для тщательного исследования выдвинутой гипотезы. Данная методология выходит за рамки поверхностного анализа и предлагает разностороннее понимание проблемы и ее потенциальных решений, необходимых для создания надежной правовой базы в области искусственного интеллекта. Преимущество использованной методологии заключается в целостном подходе, который позволяет принимать теоретически обоснованные и практически жизнеспособные решения.

3. Результаты и обсуждение

3.1. Анализ по методу PESTEL

Чисто количественные методы в стратегическом планировании редко дают явное преимущество, необходимое для проверки гипотезы. Качественные методы хорошо подходят для измерения внутренней эффективности или оценки рыночных тенденций, но их потенциал для получения более широкой картины весьма ограничен. Метод PESTEL, напротив, прекрасно подходит для систематического изучения политических, экономических, социальных, технологических, экологических и правовых факторов, давая целостное представление о внешних причинах, способствующих успеху компании (Yüksel, 2012). Этот подход отражает динамику систем искусственного интеллекта и обеспечивает всестороннее понимание потенциальных угроз и возможностей, связанных с гипотезой.

На рис. 1 показано сравнение конкретных разделов и статей законов, а также наказаний, предусмотренных законодательством разных стран. Дальнейший анализ будет основываться на этом сравнении. В табл. 1 представлен всесторонний анализ по методу PESTEL законов об ответственности за качество продукции и о халатности в различных странах.

Рис. 1. Сравнение действующих законов разных стран

Таблица 1. Анализ по методу PESTEL существующих законов об ответственности за качество продукции и о халатности в различных странах

Факторы	США	Великобритания	Индия	Китай	Россия
Политические	1. Политические изменения в интересах потребителей	1. Стабильная политическая база, мощная поддержка прав потребителей	1. Растущее внимание к защите прав потребителей	1. Централизованная политическая власть позволяет быстро вносить изменения в нормативные акты	1. Сильная политическая воля к защите прав потребителей, иногда непоследовательная реализация
	2. Противоречия между интересами потребителей, производителей и правовой системы	2. Изменения в законодательстве в связи с выходом Великобритании из Евросоюза	2. Бюрократические препоны при реализации мер	2. Твердая воля правительства к технологическому прогрессу при одновременной защите прав потребителей	2. Государственный контроль над системами
Экономические	1. Высокие судебные издержки	1. Расходы на соблюдение нормативных требований	1. Расходы на компенсации и штрафы	1. Экономические санкции негативно сказываются на бизнесе	1. Значительные экономические штрафы и санкции за причинение ущерба
	2. Высокие экономические стимулы для соблюдения требований	2. Негативное экономическое воздействие на бизнес из-за изъятия продукции и компенсаций	2. Более низкие судебные издержки по сравнению с западными странами	2. Высокие расходы на соблюдение нормативных требований и строгие законы о безопасности продукции	2. Приостановление предпринимательской деятельности при несоблюдении требований

Окончание табл. 1

Факторы	США	Великобритания	Индия	Китай	Россия
Социальные	1. Высокая осведомленность и активность потребителей	1. Мощные движения за права потребителей	1. Усилия средств массовой информации и правительства играют ключевую роль в повышении осведомленности потребителей	1. Растущие требования к продукции и высокий уровень осведомленности потребителей	1. Растущая осведомленность и активность потребителей
	2. Коллективные иски – мощный инструмент защиты прав потребителей	2. Высокая осведомленность общественности о безопасности и требованиях к продукции	2. Запрос общественности на введение строгих правил	2. Влияние социальных сетей на общественное мнение и нормативное регулирование	2. Растущий запрос общественности на ужесточение и эффективное применение норм
Технологические	1. Развитие технологий влияет на безопасность продукции	1. Высокотехнологические инновации влияют на безопасность продукции	1. Технологические достижения влияют на безопасность продукции	1. Стремительный рост в области искусственного интеллекта и бытовой электроники	1. Технологические достижения в области производства и безопасности продукции
	2. Расширение использования искусственного интеллекта для мониторинга соответствия требованиям и обнаружения дефектов	2. Внедрение искусственного интеллекта и интернета вещей для обеспечения соответствия нормативным требованиям	2. Растущее использование искусственного интеллекта для регулирования	2. Интеграция технологий мер и регулирования	2. Новейшие технологические решения в сфере регулирования
Экологические	1. Экологические аспекты ответственности за качество продукции	1. Строгие экологические нормы, влияющие на стандарты продукции	1. Ужесточение экологических требований для различных видов продукции	1. Строгие законы об охране окружающей среды, регулирующие производство продукции	1. Соблюдение экологических требований при производстве продукции
	2. Акцент на соблюдении экологической чистоты и устойчивости продукции	2. Акцент на соблюдении экологической устойчивости	2. Усилия по снижению вредного воздействия продукции на окружающую среду	2. Особое внимание правительства к экологической чистоте и устойчивости продукции	2. Особое внимание к соблюдению экологических стандартов в отношении продукции
Правовые	1. Комплексная система для юридических аспектов производства	1. Строгая ответственность в соответствии с Законом о защите прав потребителей от 1987 г.	1. Закон о защите прав потребителей от 2019 г. с множеством положений об ответственности за качество продукции	1. Положения о строгой ответственности в Законе о качестве продукции и законодательстве о гражданско-правовой ответственности	1. Строгая ответственность за качество продукции и халатность в соответствии с Гражданским кодексом и Законом о защите прав потребителей
	2. Строгая ответственность и четко определенные компенсационные и карательные нормы	2. Серьезные компенсации за ущерб, изъятие продукции	2. Штрафы, компенсации и тюремное заключение за нарушения	2. Возмещение ущерба, административные штрафы и изъятие продукции	2. Компенсации за ущерб и моральный ущерб, а также приостановление деятельности в качестве наказания

Анализ по методу PESTEL демонстрирует сложную глобальную систему ответственности за качество продукции, особенно в сфере искусственного интеллекта. США, Великобритания, Китай и Россия заявляют о наличии широкой правовой базы в области производства продукции, тогда как в Индии имеются проблемы с правоприменением. В США и Великобритании наблюдается сильная политическая поддержка защиты прав потребителей. С экономической точки зрения американские компании обременены высокими судебными издержками, в то время как Индия сталкивается с необходимостью соблюдения требований законодательства. Технологические достижения в Великобритании, США и Китае способствуют соблюдению требований, однако в некоторых регионах пробелы в правоприменении достаточно очевидны.

США и Великобритания устанавливают высокую планку благодаря строгим экологическим нормам, однако в общемировом масштабе их соблюдение осуществляется по-разному. Растущий всеобщий интерес к безопасности потребителей позволяет согласовать правовые стандарты, но разработка различных версий и мер создает риски.

Анализ также выявил очевидные возможности для глобального регулирования безопасности продукции, особенно для систем искусственного интеллекта. Эти меры основаны на повышении осведомленности потребителей и их внимания к технологическим достижениям. Для подтверждения нашей гипотезы был проведен анализ по методу PESTEL. Можно предположить, что в сфере борьбы с преступлениями, связанными с использованием искусственного интеллекта, даже гибридное применение законов об ответственности за качество продукции и законов о халатности не избавляет от необходимости точной настройки в соответствии с этими основными нормами. Существующие законы были разработаны для физических продуктов и не полностью охватывают проблемы систем с искусственным интеллектом. Проблемы правоприменения и быстрые темпы развития в области искусственного интеллекта также препятствуют эффективности обычных нормативных актов. В этих условиях только новая целостная структура будет способствовать согласованию глобальных стандартов в отношении преступлений, связанных с использованием искусственного интеллекта. Для обеспечения последовательного применения во всех странах мира такая система должна устанавливать режимы ответственности, специфичные для ИИ, обеспечивать прозрачность и опираться на глубокое понимание работы систем искусственного интеллекта.

3.2. Анализ первопричин

Анализ первопричин (Root Cause Analysis, RCA) служит важным инструментом для проверки гипотезы, особенно когда речь идет о многогранных явлениях (Barsalou, 2014). Этот метод позволяет систематически исследовать причинно-следственную связь для любого наблюдаемого явления. Тем самым можно выявить недостатки в гипотезе и внести коррективы, необходимые для обеспечения точности принятого плана исследования (Barsalou, 2014). Этот конвергентный процесс повышает надежность исследования в целом и способствует получению более существенных выводов.

На рис. 2 показана диаграмма Исикавы (схема причинно-следственных связей), показывающая неэффективность существующих законов об ответственности за качество продукции и о халатности в борьбе с преступлениями, связанными с использованием искусственного интеллекта.

Схема наглядно демонстрирует, что быстрое развитие технологий искусственного интеллекта, несоответствие им существующих нормативных актов, отсутствие прозрачности и подотчетности, а также отсутствие глобально приемлемого механизма правоприменения делают существующую систему законов об ответственности за качество продукции и о халатности неэффективной для борьбы с преступлениями, связанными с использованием искусственного интеллекта.

Методика «пять почему» – это мощный инструмент, позволяющий с помощью минимальных ресурсов выявить первопричину проблем (Barsalou & Starzynska, 2023). Он используется в различных дисциплинах и позволяет получить структурированный и логичный ответ о важнейших факторах, влияющих на состояние вопроса (Pugna et al., 2016). Повторное применение данного инструмента отсекает все поверхностные факторы, выявляя наиболее глубокую причину изучаемой проблемы.

Рис. 2. Причинно-следственные связи, показывающие неэффективность существующих законов об ответственности за качество продукции и о халатности в борьбе с преступлениями, связанными с использованием искусственного интеллекта

На рис. 3 показан систематический анализ неэффективности законов об ответственности за качество продукции в отношении преступлений, связанных с использованием искусственного интеллекта, по методу «Пять почему», а на рис. 4 – аналогичный анализ неэффективности законов о халатности.

Анализ по методу «пять почему» показывает, что действующие законы об ответственности за качество продукции и о халатности неэффективны в отношении уникальных и непредвиденных преступлений, связанных с использованием искусственного интеллекта. Это опровергает нашу гипотезу. Стремительный технологический прогресс и динамика мирового рынка превосходят адаптивные способности существующих правовых систем. В результате возникают такие явления, как недостаточность принятых стандартов, несовершенное регулирование, неудовлетворительность судебной экспертизы, недостаточная осведомленность потребителей, коммерческое использование правовых лазеек, юрисдикционные проблемы, огромные задержки судебных процедур, изменения в восприятии рисков, недостаточное финансирование судебных и регулирующих органов, а также экономическое давление, при котором интересы бизнеса ставятся выше защиты прав потребителей. Таковы основные проблемы, требующие оперативного решения и корректировки для эффективного использования существующих законов об ответственности за качество продукции и законов о халатности в целях борьбы с преступлениями, связанными с использованием искусственного интеллекта.

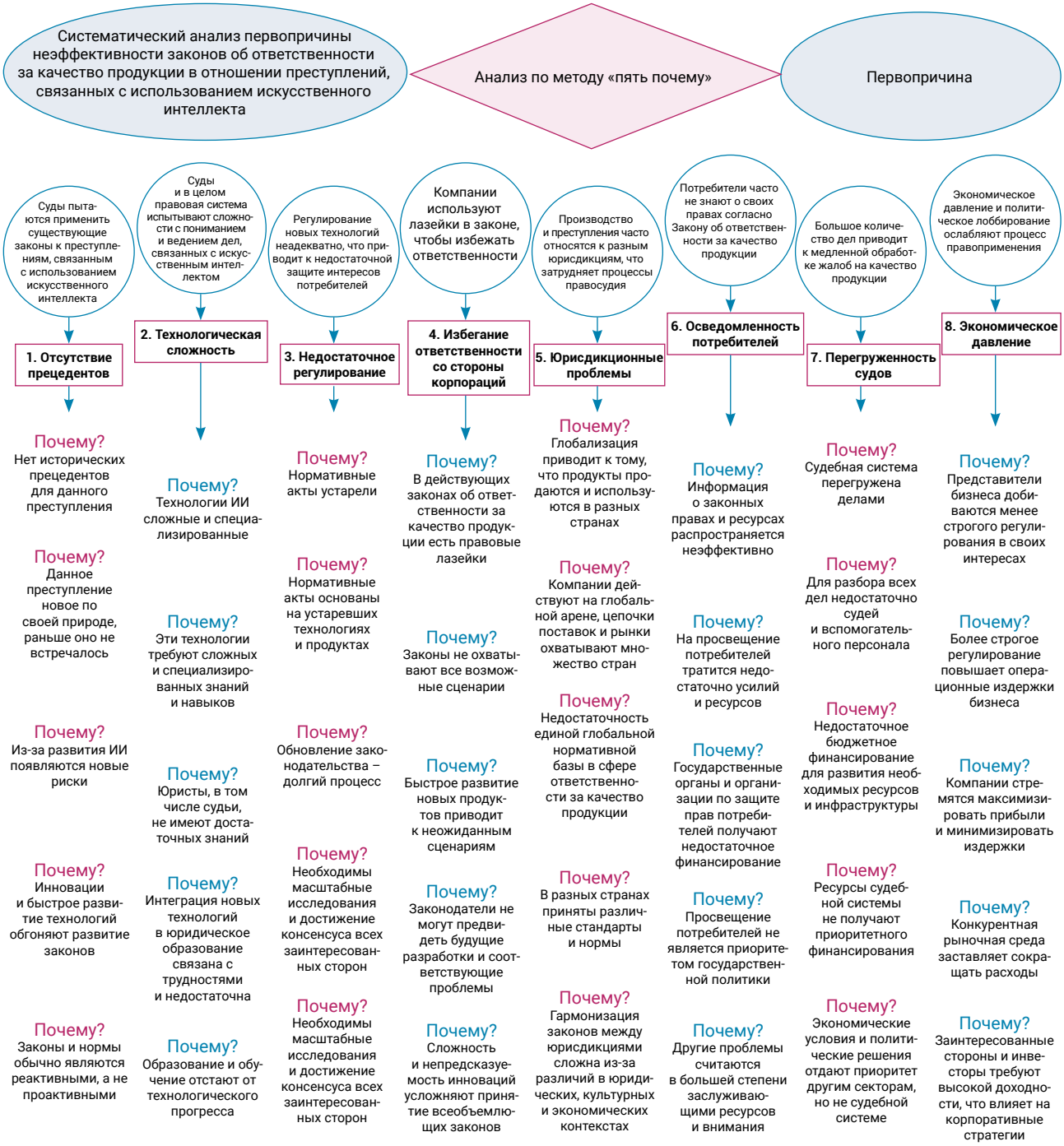


Рис. 3. Первопричины неэффективности законов об ответственности за качество продукции в отношении преступлений, связанных с использованием искусственного интеллекта

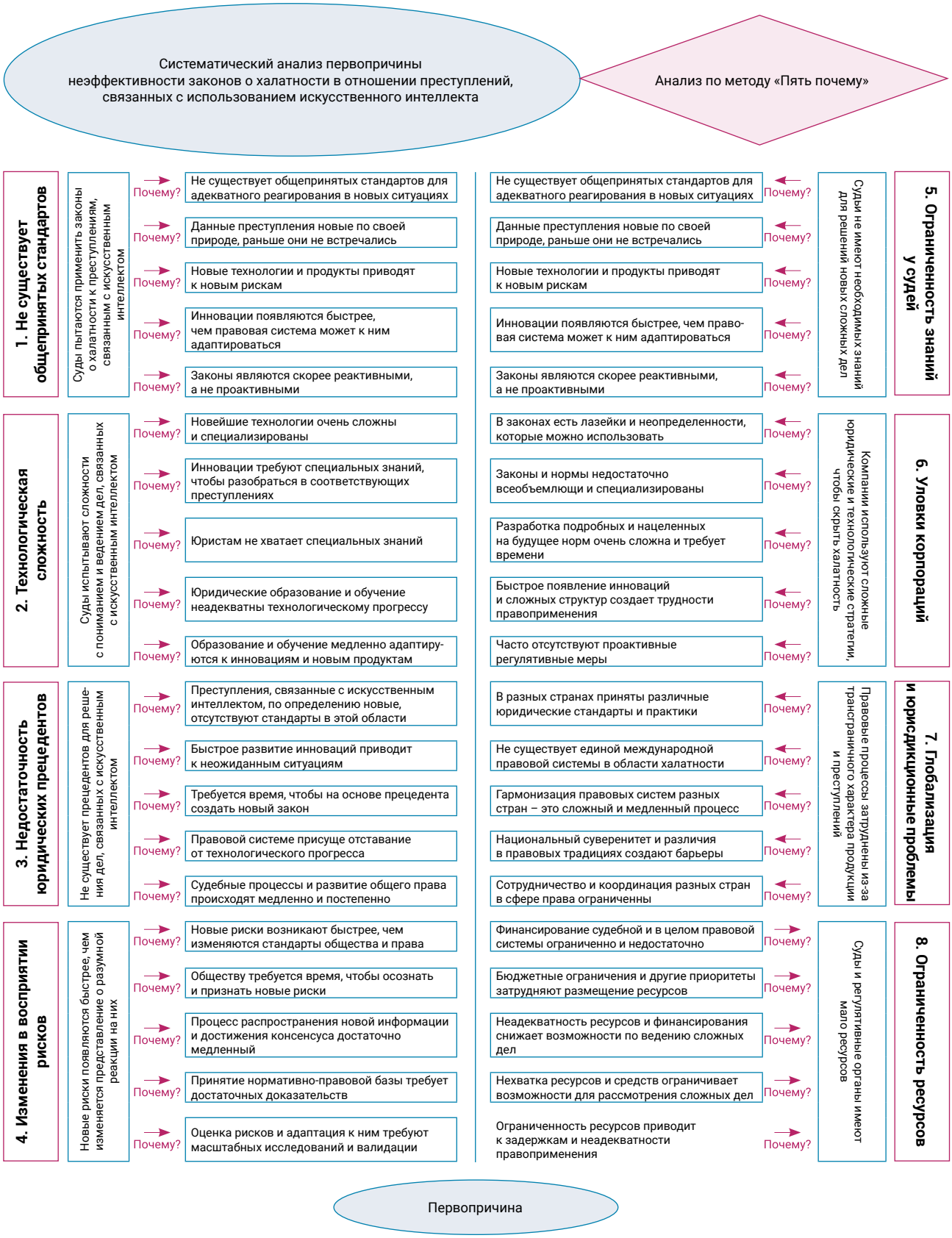


Рис. 4. Первопричины неэффективности законов о халатности в отношении преступлений, связанных с использованием искусственного интеллекта

3.3. Анализ кейсов: как в разных странах борются с преступлениями, совершенными с использованием искусственного интеллекта

3.3.1. Инцидент Greyball в США

В этом деле компания Uber использовала Greyball – инструмент на основе искусственного интеллекта, – чтобы скрывать свою деятельность от правоохранительных органов в городах, где услуги компании не были разрешены[11]. Программа идентифицировала сотрудников правоохранительных органов и выдавала им поддельную версию приложения, чтобы они не могли обнаружить машины компании. В связи с этим нарушением Департамент юстиции США и ряд местных органов власти инициировали расследование в отношении Uber. Компания согласилась прекратить использование данного инструмента и понесла репутационный ущерб. Контроль со стороны регулирующих органов был усилен. Это классический случай, когда регулирующие органы сталкиваются с преднамеренными неправомерными действиями систем искусственного интеллекта. Власти налагают штрафные санкции, которые должны послужить сдерживающим фактором для подобных действий в будущем.

3.3.2. Инцидент с нарушением конфиденциальности данных на сайте авиакомпании British Airways

В 2018 г. с веб-сайта компании British Airways, использующего системы искусственного интеллекта, произошла утечка, в результате которой были скомпрометированы личные и финансовые данные более 400 тысяч клиентов[12]. По мнению Управления комиссара по информации (ICO), компания проявила халатность в защите данных клиентов. Первоначально речь шла о выплате штрафа в размере 183 млн фунтов стерлингов, однако за сотрудничество со следствием компания была оштрафована всего на 20 млн фунтов стерлингов. Это типичный случай, когда вместо наложения сурового наказания власти предпочли установить разумные и соразмерные штрафы, чтобы поощрить применение мер саморегулирования.

3.3.3. Утечка данных из системы Aadhaar в Индии

Нарушения безопасности и халатность в управлении базами данных на основе искусственного интеллекта привели к утечке личной информации миллионов граждан через Aadhaar – систему биометрической идентификации в Индии[13]. В связи с этим индийское Управление по уникальной идентификации (UIDAI) подверглось серьезной критике и судебным разбирательствам. В дальнейшем были введены более строгие нормы соблюдения требований и усилены функции безопасности. Однако из-за существующих правовых рамок этот инцидент не повлек за собой каких-либо финансовых санкций. Этот пример подчеркивает необходимость надежной системы для эффективной борьбы с непреднамеренным ущербом, причиняемым системами искусственного интеллекта.

---

11 Greyball: how Uber used secret software to dodge the law. (2017, March 4). The Guardian. https://clck.ru/3Gq9ZC

12 BA fined record £20m for customer data breach. (2020, October 16). The Guardian. https://clck.ru/3Gq9d8

13 Aadhaar data leak exposes cyber security flaws. (2023, March 29). The Hindu Business Line. https://clck.ru/3Gq9hv

3.3.4. Инцидент с созданием дипфейков компанией Tencent в Китае

В течение 2019 г. компании Tencent пришлось столкнуться с серьезными проблемами в связи с использованием инструмента для создания дипфейков на основе ИИ. Было высказано мнение, что этот инструмент использовался для мошенничества и дезинформации. В результате были приняты срочные меры в области регулирования. Китай ввел новые правила в отношении технологий искусственного интеллекта и дипфейков. Новые правила требуют четкой маркировки и ограничения неправомерного использования этих технологий. Компания Tencent выполнила требования, внеся коррективы в функционал своего инструмента. Это уникальный пример активного использования законодательных мер, направленных на то, чтобы усилия по регулированию и цензурированию контента опережали появление новых технологий искусственного интеллекта, а также пример ужесточения правоприменения для предотвращения преднамеренных нарушений и неправомерного использования технологий искусственного интеллекта[14].

3.3.5. Российская Национальная стратегия развития искусственного интеллекта

Россия объявила о планах по предотвращению доминирования Запада в сфере технологий искусственного интеллекта[15]. Доминирование определенных стран в разработке искусственного интеллекта потенциально отражает региональные особенности, что может привести к цифровой дискриминации и негативно сказаться на суверенитете страны. Принятая Россией стратегия развития искусственного интеллекта уникальна тем, что направлена на сохранение национальной идентичности и культурного наследия при развитии технологий искусственного интеллекта. В России, в отличие от США и Великобритании, разработкой руководит не правительство или частный сектор, а государственные компании (Petrella et al., 2021). С помощью «цифровых песочниц» Россия ввела новый экспериментальный правовой режим для разработки ИИ, в рамках которого компаниям разрешается работать с системами искусственного интеллекта, которые в настоящее время не регулируются действующим законодательством. Это дает возможность этим компаниям увидеть, как разработанный ИИ работает в реальных ситуациях в Москве, а затем и по всей России[16].

3.4. Основные наблюдения и выводы

Анализ по методу PESTEL, анализ первопричины и исследование кейсов показали, что выдвигаемая гипотеза не подтверждается в случаях сложных преступлений, связанных с технологиями искусственного интеллекта. Учитывая сложность таких преступлений, применение гибридного подхода на основе существующих структур является чрезвычайно сложной задачей. Для борьбы с указанными преступлениями следует

---

14 Kharpal, A. (2022, Dec 22). China is about to get tougher on deepfakes in an unprecedented way. Here's what the rules mean. CNBC. https://clck.ru/3GqAah

15 Putin to boost AI in Russia to Fight 'Unacceptable and Dangerous' Western Monopoly. (2023, November 24). VAO. https://clck.ru/3GqAsU

16 Mondaq. https://clck.ru/3GqAyM

создать надежную международную структуру, которая бы учитывала ряд спорных вопросов. Во-первых, эта структура должна четко определять все существующие и потенциальные преступления, связанные с технологиями искусственного интеллекта. Во-вторых, она должна содержать широкий набор действий и процедур для органов прокуратуры. В-третьих, она должна предусматривать суровые наказания за преступное поведение, соответствующие быстрым темпам технологического развития и динамике мирового рынка, с включением традиционных элементов mens rea и actus reus. Система должна способствовать правоприменению и соблюдению требований, оставаясь при этом справедливой по отношению к ответчикам, а также повышать информированность клиентов. Правовые нормы должны способствовать достижению согласия между национальными и международными органами и повышать эффективность юрисдикций в целях обеспечения правосудия, подотчетности и прав всех заинтересованных сторон.

Чтобы лучше понять уровень проблем, создаваемых развивающимися системами ИИ, рассмотрим еще ряд идей, почерпнутых из различных областей. Так, ИИ часто сравнивают с оружием, поскольку человек несет ответственность за его использование. Эта идея не выдерживает юридической проверки, так как последствия интенсивного развития ИИ непредсказуемы. Другой возможный подход к регулированию ИИ – возложить «строгую ответственность» на разработчиков и придать субъектность определенным системам искусственного интеллекта. Однако такие системы ИИ создаются для того, чтобы развиваться и принимать собственные решения, что чрезвычайно затрудняет регулирование ИИ. Еще одна идея состоит в том, чтобы рассматривать непредвиденное и непреднамеренное действие ИИ по аналогии с «обстоятельствами непреодолимой силы», так как в них также отсутствует критерий намерения. Эта идея привела к важным выводам, таким как принятие упреждающих мер, проверки безопасности и разработка этических принципов для искусственного интеллекта. С другой стороны, регулируя ИИ таким же образом, каким власти борются с инфекционными заболеваниями, можно найти сходство в управлении рисками и просвещении общественности. Однако этой концепции не хватает целенаправленности и высоких темпов изменений, которые обычно ассоциируются с ИИ. Наконец, можно регулировать ИИ способом, аналогичным регулированию в области ядерного оружия, когда особое внимание уделяется международному сотрудничеству и соблюдению надлежащих норм безопасности, не забывая при этом о проблемах, связанных с доступностью и быстрым развитием систем ИИ.

Из вышеизложенного следует, что нам следует сосредоточиться на объяснимом ИИ, надежных стандартах безопасности, постепенном совершенствовании надзора и адаптации законодательной базы. Это помогло бы обеспечить ответственность человека на всех этапах разработки и внедрения ИИ. Целью должно быть создание ответственной системы искусственного интеллекта с четким распределением обязанностей и возможностью принять адекватные упреждающие меры для минимизации риска непредвиденного ущерба и обеспечения того, чтобы искусственный интеллект оставался инструментом во благо.

Создание такой системы является трудоемкой задачей, которая становится еще более сложной, поскольку необходимо достичь прочного консенсуса разных стран для ее эффективного применения в отношении преступлений, совершаемых с помощью систем искусственного интеллекта, за пределами конкретной юрисдикции. До тех пор все страны, разрешающие использование технологий искусственного

интеллекта, должны адаптировать свою существующую правовую базу для решения проблемы преступлений, связанных с использованием искусственного интеллекта. Такая адаптация должна происходить преимущественно в форме следующих мер:

1. Модернизация определения преступления с целью включения в него преступлений, связанных с ИИ, как умышленных, так и непреднамеренных.
2. Установление основных принципов разработки и внедрения ИИ.
3. Поэтапное внедрение норм в области ИИ, начиная с четких руководящих принципов, развивающихся параллельно с достижениями в области ИИ.
4. Поощрение разработчиков к созданию исключительно прозрачных и объяснимых систем искусственного интеллекта.
5. Обязательное публичное раскрытие информации и сотрудничество с целью учета социальных и этических аспектов при разработке нормативной базы.
6. Обязательные требования по повышению осведомленности общественности о разработчиках и пользователях ИИ.
7. Создание независимых специализированных органов для мониторинга разработки и внедрения ИИ.
8. Обязательное финансирование исследований в области объяснимого ИИ, разработка стандартов безопасности и изучение последствий ИИ для общества.

Заключение

Данное исследование направлено на изучение целесообразности гибридного применения существующего Закона об ответственности за качество продукции и Закона о халатности в отношении преступлений, связанных с искусственным интеллектом. Систематическая работа с использованием таких методов, как PESTEL, анализ первопричины и исследование кейсов, позволила автору углубленно изучить гипотезу и получить ценную информацию о требованиях законодательной базы для систем искусственного интеллекта.

Обеспечение подотчетности ИИ сопряжено со многими сложностями. Ответственность программиста остается ключевым аспектом, однако постоянно развивающиеся системы ИИ говорят о необходимости многоуровневой структуры. Уникальные возможности ИИ требуют уникального подхода. Технологии искусственного интеллекта все чаще используются в общемировом масштабе, и для того, чтобы ИИ приносил пользу обществу, необходимы международное сотрудничество, надежные стандарты безопасности и постоянная адаптация. Важно сосредоточиться на основных принципах регулирования, наладить поэтапное внедрение и уделять приоритетное внимание прозрачности, подотчетности и активным мерам, таким как просвещение общественности, наличие специализированных регулирующих органов и достаточных средств для продолжения исследований в области ответственного ИИ. Это, безусловно, обеспечит такое будущее, в котором ИИ будет служить человечеству только во благо.

Настоящее исследование основано на высоконаучном, качественном, беспрецедентном подходе к решению проблемы разработки нормативно-правовой базы для ИИ, что позволило сделать обоснованные выводы. Работа вносит существенный вклад в науку, предлагая соответствующие идеи и меры для создания надежной системы ИИ. Будущие исследования в области объяснимого ИИ и разработка стандартов безопасности обеспечат более полное понимание необходимого регулирования в области искусственного интеллекта.

Список литературы

Ли, Яо. (2023). Особенности нормативно-правового регулирования генеративного искусственного интеллекта в Великобритании, США, Евросоюзе и Китае. *Право. Журнал Высшей школы экономики*, *16*(3), 245–267. EDN: https://elibrary.ru/yitzoa. DOI: https://doi.org/10.17323/2072-8166.2023.3.245.267

Шестак, В. А., Волеводз, А. Г., Ализаде, В. А. (2019). О возможности доктринального восприятия системой общего права искусственного интеллекта как субъекта преступления: на примере уголовного законодательства США. *Всероссийский криминологический журнал*, *13*(4), 547–554. https://doi.org/10.17150/2500-4255.2019.13(4).547-554

Abbott, R., & Sarch, A. (2019). Punishing Artificial Intelligence: Legal Fiction or Science Fiction. *UC Davis Law Review*, *53*, 323–384. https://doi.org/10.2139/SSRN.3327485

Barsalou, M. A. (2014). *Root cause analysis: A step-by-step guide to using the right tool at the right time*. New York: CRC Press. https://doi.org/10.1201/b17834

Barsalou, M., & Starzyńska, B. (2023). Inquiry into the Use of Five Whys in Industry. *Quality Innovation Prosperity*, *27*(1), 62–78. https://doi.org/10.12776/qip.v27i1.1771

Bhatt, N., & Bhatt, J. (2023). Towards a Novel Eclectic Framework for Administering Artificial Intelligence Technologies: A Proposed 'PEEC' Doctrine. *EPRA International Journal of Research and Development (IJRD)*, *8*(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888

Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, *31*(4), 543–556. https://10.1007/s13347-017-0263-5

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3407779

Calo, R. (2019). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, *51*(2), 399–435. https://dx.doi.org/10.2139/ssrn.3015350

Dremliuga, R., & Prisekina, N. (2020). The Concept of Culpability in Criminal Law and AI Systems. *Journal of Programming Languages*, *13*(3), 256. https://doi.org/10.5539/jpl.v13n3p256

Gless, S. (2019). AI in the Courtroom: a comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, *51*(2), 195–253.

Ivan, D., & Manea, T. (2022). AI Use in Criminal Matters as Permitted Under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. *International Journal of Law in Changing World*, *1*(1), 17–32. https://doi.org/10.54934/ijlcw.v1i1.15

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*, 389–399. https://doi.org/10.1038/s42256-019-0088-2

Khan, K., Ali, A., Khan, Z., & Siddiqua, H. (2021). Artificial Intelligence and Criminal Culpability. In *2021 International Conference on Innovative Computing (ICIC), IEEE* (pp. 1–7). https://doi.org/10.1109/icic53490.2021.9692954

Khisamova, Z., & Begishev, I. (2019). Criminal Liability and Artificial Intelligence: Theoretical and Applied Aspects. *Russian Journal of Criminology*, *13*(4), 564–574. https://doi.org/10.17150/2500-4255.2019.13(4).564-574

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In J. Cowls, & J. Morley (Eds.), *The 2020 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*. Springer, Cham. https://doi.org/10.1007/978-3-030-80083-3_14

Kingston, J. K. (2016). Artificial Intelligence and Legal Liability. In M. Bramer, & M. Petridis (Eds.), *Research and Development in Intelligent Systems XXXIII. SGAI 2016*. Springer, Cham. https://doi.org/10.1007/978-3-319-47175-4_20

Lagioia, F., & Sartor, G. (2019). AI Systems under Criminal Law: A Legal Analysis and A Regulatory Perspective. *Philosophy & Technology*, *33*, 433–465. https://doi.org/10.1007/s13347-019-00362-x

Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: the role of state-owned firms. *Orbis*, *65*(1), 75–100. https://doi.org/10.1016/j.orbis.2020.11.004

Pugna, A., Negrea, R., & Miclea, S. (2016). Using Six Sigma Methodology to Improve the Assembly Process in an Automotive Company. *Procedia – Social and Behavioral Sciences*, *221*, 308–316. https://doi.org/10.1016/J.SBSPRO.2016.05.120

Qatawneh, I., Moussa, A., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, *12*(1), 143–150. https://doi.org/10.36941/ajis-2023-0012

Scherer, M. U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, *29*(2), 353. https://doi.org/10.2139/ssrn.2609777

Solum, L. B. (2020). Legal personhood for artificial intelligences. In *Machine ethics and robot ethics* (pp. 415–471). Routledge.

Sukhodolov, A., Bychkov, A., & Bychkova, A. (2020). Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects. *Journal of Siberian Federal University*, *13*(1), 116–122. https://doi.org/10.17516/1997-1370-0542

Yüksel, I. (2012). Developing a Multi-Criteria Decision Making Model for PESTEL Analysis. *International Journal of Biometrics*, *7*(24), 52. https://doi.org/10.5539/IJBM.V7N24P52

Zhao, S. (2024). *Principle of Criminal Imputation for Negligence Crime Involving Artificial Intelligence*. Springer Nature. https://10.1007/978-981-97-0722-5

Сведения об авторе

Бхатт Нилкант – PhD в области инженерных наук, кафедра гражданского проектирования, Инженерный колледж Лухдхирджи, г. Морби, Индия
Адрес: Индия, 363642, г. Морби, Гуджарат, Сама Канте
E-mail: neelkanth78bhatt@gmail.com
ORCID ID: https://orcid.org/0000-0003-0315-2985
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024
Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Благодарность

Автор выражает благодарность господину Джайкишен Бхатт, сотруднику Службы социального обеспечения в отставке (Государственная корпорация страхования работников, Ахмадабад, Гуджарат, Индия) и господину Бипин Пандит, профессору гражданского строительства в отставке (Инженерный колледж Лухдхирджи, Морби, Гуджарат, Индия) за их квалифицированную помощь в формулировании, написании и тщательной корректуре работы, что значительно повысило ее точность и качество.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.77 / Уголовное право
Специальность ВАК: 5.1.4 / Уголовно-правовые науки

История статьи

Дата поступления – 2 сентября 2024 г.
Дата одобрения после рецензирования – 20 сентября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:343.3/.7:004.056:004.9
EDN: https://elibrary.ru/rtolza
DOI: https://doi.org/10.21202/jdtl.2025.3

Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era

Neelkanth Bhatt

Lukhdhirji Engineering College, Morbi, India

Keywords

artificial intelligence,
crime,
criminal legislation,
criminal liability,
criminality,
digital technologies,
law,
PESTEL technique,
product quality,
security

Abstract

Objective: to study the applicability of existing norms on product quality liability and negligence laws to crimes related to artificial intelligence. The author hypothesizes that the hybrid application of these legal mechanisms can become the basis for an effective regulatory system under the rapid technological development.

Methods: the research includes a comprehensive approach based on the PESTEL analysis (political, economic, social, technological, environmental and legal factors), the "five whys" root cause analysis, and cases from various countries. This multi-level approach allows not only identifying key problems, but also proposing adapted solutions that take into account the specifics of crimes related to artificial intelligence.

Results: the research shows that the existing norms on product quality and negligence are not effective enough to regulate crimes related to artificial intelligence. The main obstacles are technological complexity, lack of precedents, lack of consumer awareness, and jurisdictional issues. The author concludes that effective regulation requires a global system that includes clear principles of responsibility, strict safety standards, and constant adaptation to new challenges.

Scientific novelty: the paper represents a unique approach to the crimes related to artificial intelligence through the prism of hybrid application of existing legal mechanisms. It offers a new perspective on the problem, combining theoretical analysis with practical recommendations based on case study.

Practical significance: recommendations for legislators and regulators were developed. The author emphasizes the need to create specialized agencies, introduce educational programs for citizens and employees, and to provide funding for research in the field of explicable artificial intelligence and security standards. These measures are aimed at forming a stable regulatory system capable of effectively countering crimes related to the use of artificial intelligence. The work opens up new horizons for further research on the regulation of AI technologies and emphasizes the need for international cooperation and an interdisciplinary approach.

For citation

Bhatt, N. (2025). Crimes in the Age of Artificial Intelligence: a Hybrid Approach to Liability and Security in the Digital Era. *Journal of Digital Technologies and Law, 3*(1), 65–88. https://doi.org/10.21202/jdtl.2025.3

References

Abbott, R., & Sarch, A. (2019). Punishing Artificial Intelligence: Legal Fiction or Science Fiction. *UC Davis Law Review*, *53*, 323–384. https://doi.org/10.2139/SSRN.3327485

Barsalou, M. A. (2014). *Root cause analysis: A step-by-step guide to using the right tool at the right time*. New York: CRC Press. https://doi.org/10.1201/b17834

Barsalou, M., & Starzyńska, B. (2023). Inquiry into the Use of Five Whys in Industry. *Quality Innovation Prosperity*, *27*(1), 62–78. https://doi.org/10.12776/qip.v27i1.1771

Bhatt, N., & Bhatt, J. (2023). Towards a Novel Eclectic Framework for Administering Artificial Intelligence Technologies: A Proposed 'PEEC' Doctrine. *EPRA International Journal of Research and Development (IJRD)*, *8*(9), 27–36. https://doi.org/10.13140/RG.2.2.11434.18888

Binns, R. (2018). Algorithmic accountability and public reason. *Philosophy & Technology*, *31*(4), 543–556. https://10.1007/s13347-017-0263-5

Broadhurst, R., Maxim, D., Brown, P., Trivedi, H., & Wang, J. (2019). Artificial Intelligence and Crime. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3407779

Calo, R. (2019). Artificial intelligence policy: A primer and roadmap. *UC Davis Law Review*, *51*(2), 399–435. https://dx.doi.org/10.2139/ssrn.3015350

Dremliuga, R., & Prisekina, N. (2020). The Concept of Culpability in Criminal Law and AI Systems. *Journal of Programming Languages*, *13*(3), 256. https://doi.org/10.5539/jpl.v13n3p256

Gless, S. (2019). AI in the Courtroom: a comparative analysis of machine evidence in criminal trials. *Georgetown Journal of International Law*, *51*(2), 195–253.

Ivan, D., & Manea, T. (2022). AI Use in Criminal Matters as Permitted Under EU Law and as Needed to Safeguard the Essence of Fundamental Rights. *International Journal of Law in Changing World*, *1*(1), 17–32. https://doi.org/10.54934/ijlcw.v1i1.15

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*, 389–399. https://doi.org/10.1038/s42256-019-0088-2

Khan, K., Ali, A., Khan, Z., & Siddiqua, H. (2021). Artificial Intelligence and Criminal Culpability. In *2021 International Conference on Innovative Computing (ICIC), IEEE* (pp. 1–7). https://doi.org/10.1109/icic53490.2021.9692954

Khisamova, Z., & Begishev, I. (2019). Criminal Liability and Artificial Intelligence: Theoretical and Applied Aspects. *Russian Journal of Criminology*, *13*(4), 564–574. https://doi.org/10.17150/2500-4255.2019.13(4).564-574

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2021). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. In J. Cowls, & J. Morley (Eds.), *The 2020 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook*. Springer, Cham. https://doi.org/10.1007/978-3-030-80083-3_14

Kingston, J. K. (2016). Artificial Intelligence and Legal Liability. In M. Bramer, & M. Petridis (Eds.), *Research and Development in Intelligent Systems XXXIII. SGAI 2016*. Springer, Cham. https://doi.org/10.1007/978-3-319-47175-4_20

Lagioia, F., & Sartor, G. (2019). AI Systems under Criminal Law: A Legal Analysis and A Regulatory Perspective. *Philosophy & Technology*, *33*, 433–465. https://doi.org/10.1007/s13347-019-00362-x

Li, Yao (2023). Specifics of Regulatory and Legal Regulation of Generative Artificial Intelligence in the UK, USA, EU and China. Law. *Journal of the Higher School of Economics*, *16*(3), 245–267 (in Russ.). https://doi.org/10.17323/2072-8166.2023.3.245.267

Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: the role of state-owned firms. *Orbis*, *65*(1), 75–100. https://doi.org/10.1016/j.orbis.2020.11.004

Pugna, A., Negrea, R., & Miclea, S. (2016). Using Six Sigma Methodology to Improve the Assembly Process in an Automotive Company. *Procedia – Social and Behavioral Sciences*, *221*, 308–316. https://doi.org/10.1016/J.SBSPRO.2016.05.120

Qatawneh, I., Moussa, A., Haswa, M., Jaffal, Z., & Barafı, J. (2023). Artificial Intelligence Crimes. *Academic Journal of Interdisciplinary Studies*, *12*(1), 143–150. https://doi.org/10.36941/ajis-2023-0012

Scherer, M. U. (2015). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, *29*(2), 353. https://doi.org/10.2139/ssrn.2609777

Shestak, V., Volevodz, A., & Alizade, V. (2019). On the Possibility of Doctrinal Perception of Artificial Intelligence as the Subject of Crime in the System of Common Law: Using the Example of the U.S. Criminal Legislation. *Russian Journal of Criminology*. *13*(4), 547–554. https://doi.org/10.17150/2500-4255.2019.13(4).547-554

Solum, L. B. (2020). Legal personhood for artificial intelligences. In *Machine ethics and robot ethics* (pp. 415–471). Routledge.

Sukhodolov, A., Bychkov, A., & Bychkova, A. (2020). Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects. *Journal of Siberian Federal University*, *13*(1), 116–122. https://doi.org/10.17516/1997-1370-0542

Yüksel, I. (2012). Developing a Multi-Criteria Decision Making Model for PESTEL Analysis. *International Journal of Biometrics*, *7*(24), 52. https://doi.org/10.5539/IJBM.V7N24P52

Zhao, S. (2024). *Principle of Criminal Imputation for Negligence Crime Involving Artificial Intelligence*. Springer Nature. https://10.1007/978-981-97-0722-5

Author information

Neelkanth Bhatt – PhD (Engineering), Assistant Professor, Department of Civil Engineering, Lukhdhirji Engineering College
Address: Sama Kanthe, Morbi, Gujarat 363642, India
E-mail: neelkanth78bhatt@gmail.com
ORCID ID: https://orcid.org/0000-0003-0315-2985
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58919442100
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KRO-8652-2024
Google Scholar ID: https://scholar.google.com/citations?user=L7K-e3IAAAAJ

Conflict of interest

The author declare no conflict of interest.

Financial disclosure

The research had no sponsorship.

Acknowledgements

The author is grateful to Shri. Jaikishen Bhatt, Retired Social Security Officer, Employees' State Insurance Corporation, Ahmedabad (Gujarat, India) and Prof. Bipin Pandit, Retired Professor of Civil Engineering, Lukhdhirji Engineering College, Morbi (Gujarat, India) for their expert help with language, writing and meticulous proofreading which significantly improved the clarity and the quality of the work.

Thematic rubrics

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

Article history

Date of receipt – September 2, 2024
Date of approval – September 20, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:177.5:316.647.82:004.8:004.652
EDN: https://elibrary.ru/mbwjxf
DOI: https://doi.org/10.21202/jdtl.2025.4

Конституционно-правовой аспект создания больших языковых моделей: проблема цифрового неравенства и языковой дискриминации

Илья Геннадьевич Ильин

Санкт-Петербургский государственный университет, Санкт-Петербург, Россия

Ключевые слова

большие языковые модели,
генеративный искусственный интеллект,
искусственный интеллект,
конституционные права,
обработка естественного языка,
права человека,
право,
цифровое неравенство,
цифровые технологии,
языковая дискриминация

Аннотация

Цель: исследование влияния цифрового неравенства на реализацию конституционных прав человека, а также выявление рисков языковой дискриминации, связанных с разработкой и использованием больших языковых моделей.

Методы: формально-юридический и сравнительно-правовой методы, а также метод теоретического моделирования. Эти подходы дополняются общенаучными методами познания, что позволяет провести комплексный анализ правовых, технологических и социальных аспектов проблемы.

Результаты: было установлено, что применительно к большим языковым моделям цифровое неравенство возникает из-за неравномерного уровня цифровизации языков и проявляется в ограниченном доступе к технологии обработки естественного языка. В свою очередь, неравный доступ к указанной технологии может негативно влиять на реализацию конституционно гарантированных прав и может быть рассмотрен с точки зрения концепций «равенства» и запрета на дискриминацию. Автор подчеркивает, что неравный доступ к технологиям обработки естественного языка может усугублять существующие социальные и экономические неравенства, создавая новые формы дискриминации.

Научная новизна: заключается в анализе скрытых и косвенных форм дискриминации, которые проявляются в системах искусственного интеллекта, особенно в генеративных моделях. В отличие от прямых форм дискриминации, которые могут быть выявлены в предсказательных алгоритмах, генеративные модели создают более тонкие, но не менее значимые кумулятивные эффекты. Эти эффекты способствуют формированию социальных стереотипов и неравенства в таких областях, как профессиональная деятельность, гендерная и этническая принадлежность. Автор также обращает внимание на то, что с увеличением

автономности искусственного интеллекта традиционные подходы к выявлению дискриминации становятся менее эффективными, что требует разработки новых методов анализа и регулирования.

Практическая значимость: состоит в том в том, что его результаты предоставляют основу для выявления и оценки правовых рисков, связанных с неравным доступом к цифровым продуктам, использующим технологии обработки естественного языка. Это способствует совершенствованию правового регулирования в сфере разработки и использования технологий искусственного интеллекта. Статья предлагает рекомендации для законодателей, регулирующих органов и разработчиков технологий, направленные на минимизацию рисков цифрового неравенства и языковой дискриминации.

Для цитирования

Ильин, И. Г. (2025). Конституционно-правовой аспект создания больших языковых моделей: проблема цифрового неравенства и языковой дискриминации. *Journal of Digital Technologies and Law*, *3*(1), 89–107. https://doi.org/10.21202/jdtl.2025.4

Содержание

Введение

Большие языковые модели (англ. Large Language Models, LLM) – это генеративные модели искусственного интеллекта используемые в технологии обработки естественного языка (англ. Natural language processing, NLP). Наличие таких моделей позволяет компьютеру эффективно обрабатывать текстовые данные, демонстрируя способность к «пониманию» текста на глубоком уровне, создавать связные и контекстуально релевантные ответы на запросы, осуществлять перевод текста между языками, а также генерировать текст, который соответствует определенным стилевым и содержательным требованиям (Glauner, 2024). В качестве примеров больших языковых моделей можно, например, выделить BERT[1], GPT-3[2] и связанные с ними цифровые продукты, такие как «Гугл Ассистент» (англ. Google Assistant), «Чат ДжиПиТи» (англ. ChatGPT).

[1] Generative Pre-trained Transformer (GPT) – серия больших языковых моделей, разработанных компанией OpenAI (США). Основаны на архитектуре Transformer. Обучаются без «учителя», не требуют адаптации и могут быть использованы и адаптированы для широкого спектра задач. Подробнее о модели GPT см. (Yenduri G. et al., 2023). Подробнее об архитектуре Transformer см. (Vaswani, 2017).

[2] Bidirectional Encoder Representations from Transformers (BERT) – большая языковая модель, разработанная компанией Alphabet Inc. (США). Основана на архитектуре Transformer. Обучается на двунаправленном (bidirectional) контексте – может анализировать и «понимать» текст как слева направо, так и справа налево. Подробнее о модели BERT см. (Devlin J. et al., 2018).

Большие языковые модели обучаются на обширных массивах языковых данных, включая структурированные лингвистические корпуса: базы данных, содержащие разнообразные тексты (книги, текстовые транскрипции, переводы и т. д.) и аудиофайлы (аудиокниги, записи трансляций, подкасты, другой аудиоконтент). Структура и репрезентативность таких данных, их объем и формат определяют процесс обучения и точность понимания контекста (Ilin, 2024), а наличие дефектов[3] или недостаточность данных может приводить к некорректной работе модели и в целом препятствовать развитию технологии (Hacker, 2021). Таким образом, возможность создания качественной языковой модели будет напрямую зависеть от объема, репрезентативности и других качественных характеристик обучающих данных для соответствующего языка.

Вместе с тем уровни цифровизации языков – объем существующих лингвистических корпусов и данных для их создания – существенно отличаются друг от друга. Для некоторых языков или диалектов данные могут быть крайне ограниченными или вообще отсутствовать. Это препятствует разработке точных и эффективных языковых моделей, что замедляет их цифровое развитие и ограничивает интеграцию в современные технологии. Например, если набор данных недостаточно полон и не охватывает все варианты диалектов определенного языка, модель может неверно или неточно обрабатывать входящие запросы, а в некоторых случаях вообще не функционировать. Различия в произношении, лексике и грамматике могут приводить к ошибкам в распознавании и анализе текста или речи, снижать качество результатов.

Невозможность создания полноценной языковой модели для определенных языков или их диалектов приводит к недоступности множества цифровых продуктов для носителей этих языков или существенно ухудшает качество их работы по сравнению с тем, как те же технологии функционируют для носителей языков с высоким уровнем цифровизации. В итоге возникает цифровое неравенство, при котором доступ к современным технологиям распределяется неравномерно среди различных языковых сообществ, что, в свою очередь, усиливает риск дискриминации.

Цель настоящей статьи – проанализировать конституционно-правовые аспекты создания больших языковых моделей в контексте цифрового неравенства и языковой дискриминации. Для достижения этой цели будет исследовано, как цифровое неравенство воздействует на конституционные права человека, а также проанализированы риски языковой дискриминации, связанные с созданием больших языковых моделей.

Статья содержит основные результаты соответствующего исследования, а также направления для дальнейшего изучения проблемы. Текст предложенной исследовательской работы разделен на три тематические части, дополненные введением и заключением. В первой части анализируется проблема цифрового неравенства в контексте различного уровня цифровизации языков – объема и репрезентативности языковых данных. Вторая часть рассматривает языковую дискриминацию как потенциальную форму проявления цифрового неравенства с акцентом на проблему

[3] В данном контексте дефект данных включает в себя как несоответствие данных определенным техническим критериям и метриками (дефект качества), например критериям репрезентативности, объему, чистоте и т. д., так и дефект права – использования данных с нарушением применимого правового режима. Например, нарушение режима персональных данных при их обработке в составе языковой модели. Подробнее о влиянии качества данных на процесс создания больших языковых моделей см. (Ilin, 2024).

неравного доступа к технологиям обработки естественного языка (NLP). В третьей части проблема языковой дискриминации концептуализируется во взаимосвязи с другими правами человека и в контексте развития цифровых технологий.

1. Цифровизация языков как источник цифрового неравенства: технико-правовой анализ

Цифровое неравенство представляет собой одну из форм социального неравенства, характеризующуюся неравным доступом к информационным технологиям и различиями в уровне навыков их использования среди отдельных лиц и социальных групп (Мушаков, 2022). Это явление охватывает широкий спектр факторов, включая различия в техническом оснащении, доступ к интернет-ресурсам, уровень цифровой грамотности и образовательные возможности, что, в свою очередь, ведет к социальному и экономическому разделению (Rogers, 2016). Необходимость устранения разрывов в доступе к цифровым технологиям для достижения более равного и инклюзивного общества неоднократно отмечалась как на национальном[4], так и на международном[5] уровне.

В контексте создания больших языковых моделей проблема цифрового неравенства выражается в ограниченной возможности носителей языков с низким уровнем цифровизации использовать цифровые продукты на своем языке. Это приводит к неравному доступу отдельных людей или социальных групп к технологиям обработки естественного языка (NLP). Следствием чего могут стать ограничения в доступе к информации, образованию, социальным услугам для носителей таких языков. Например, способность контекстного понимания текста и генерации соответствующих ответов способствует активному применению этой технологии в таких сферах, как образование и здравоохранение (Jiang et al., 2023; Sohail & Zhang, 2024). Отсутствие поддержки определенных языков в данных областях может негативно сказаться на возможности реализации соответствующих конституционно гарантированных прав: права на доступ к образованию[6] и медицинской помощи[7], ограничивая доступность и качество данных услуг. В этой связи представляется логичным рассматривать проблему цифрового неравенства с точки зрения конституционно-правовых отношений: концепций «равенства» и запрета на дискриминацию[8].

---

4 Постановление Правительства РФ № 313 от 15.04.2014. (2014). Здесь и далее все ссылки на документы, нормативно-правовые акты и судебную практику приводятся по СПС «КонсультантПлюс». https://clck.ru/3GP8do

5 Декларация принципов построения информационного общества (ООН) от 12 декабря 2003 г. https://clck.ru/3GP8fD ; Тунисская программа для информационного общества (ООН) от 15 ноября 2005 г. https://clck.ru/3GP8ge

6 Конституция Российской Федерации, принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 (далее – Конституция Российской Федерации). Ст. 43. https://clck.ru/3GP8hh

7 Конституция Российской Федерации. Ст. 41. https://clck.ru/3GP8jK

8 В обоих случаях рассматривается вопрос равенства прав, однако право на недискриминацию обладает более узким содержанием и в этом смысле вытекает из общего права на равенство. Подробнее см. (Талапина, 2022).

Можно также согласиться с некоторыми исследователями, что конституционные нормы, обеспечивающие равенство перед законом и доступ к услугам, должны учитывать и устранять неравенство в доступе к цифровым ресурсам, поскольку это напрямую влияет на способность граждан реализовывать свои права и свободы в цифровую эпоху (Мушаков, 2022).

Для создания эффективной языковой модели необходим набор обучающих данных, который должен соответствовать таким критериям, как объем, репрезентативность[9], и другим качественным характеристикам. Эти параметры напрямую зависят от уровня цифровизации конкретного языка, поскольку чем выше степень цифровизации, тем более разнообразные и качественные данные могут быть использованы для обучения модели.

Цифровизация языка в широком смысле – это преобразование данных в соответствующие электронные лингвистические корпуса. Для этого используются текстовые данные (например, файлы, транскрипции, аннотации), речевые данные (например, аудиозаписи, фонетические и интонационные аннотации) и мультимодальные данные (т. е. данные, сочетающие в себе сразу несколько видов, например, видео и текстовые данные, изображения и текст и т. д.) (Dash & Arulmozi, 2018). Следует отметить, что этот процесс не только содействует развитию технологий и цифровой трансформации общества, но еще играет важную роль в сохранении национальной и культурной идентичности (Kelli et al., 2016). Например, цифровизация миноритарных языков может значительно способствовать сохранению культурного наследия малых народов.

Несмотря на важность цифровизации для технологического прогресса и высокую социальную значимость данного процесса, уровень цифровизации языков, их диалектов и наречий остается неравномерным. Можно выделить экономические, технические, а также правовые факторы, ограничивающие или препятствующие цифровизации языков.

Экономические факторы связаны с тем, что языки имеют разный экономический потенциал (Alarcón, 2022; Monteith & Sung, 2023), а процесс цифровизации требует значительных ресурсов, в том числе временных, финансовых и т. д. В этой связи разработка лингвистических корпусов для некоторых языков может оказаться экономически нецелесообразной. Технические факторы связаны непосредственно с процессом создания лингвистических корпусов. К таким факторам может отнести ошибки при сборе данных, недостатки в конструкции корпусов и ограничения существующих наборов данных, ошибки в метаданных и т. д. (Solovyev & Akhtyamova, 2019; Doğruöz et al., 2023; Li et al., 2024). Правовые факторы связаны с наличием нормативных ограничений на доступ к обучающим данным и необходимостью соблюдения соответствующего правового режима при их использовании для обучения.

В предыдущих работах автора подробно рассматривались вопросы регулирования доступа к обучающим данным (Ilin, 2024), а также соблюдения их правовых режимов, таких как режим персональных данных (Ilin, 2020) и режим объектов

[9] Учитывая многогранное значение термина «репрезентативность» (см. подробнее (Chasalow & Levy, 2021)), важно обозначить, что в контексте данной статьи под объемом языковых данных подразумевается их количество, а под репрезентативностью – их разнообразие, т. е. степень охвата различных стилей, диалектов, временных периодов и контекстов.

интеллектуальной собственности (Ilin, 2022; Ilin & Kelli, 2019, 2024). Центральной проблемой данных исследований явилась проблема конфликта между одинаково охраняемыми правами человека при использовании обучающих данных, например права на недискриминацию[10] и права на защиту неприкосновенности частной жизни, личную и семейную тайну[11]. Преодоление этой проблемы необходимо как на концептуальном уровне (устранение нормативных барьеров для доступа к данным с учетом баланса частных и публичных интересов), так и в практическом плане (создание условий для распространения и обмена языковыми данными, например, при помощи развития института повторного использования данных, накопленных в государственных информационных системах (далее – ГИС) или привлечения высших учебных заведений для создания лингвистических корпусов и цифровизации языка).

Согласно аналитическому докладу Счетной палаты РФ[12], на 2020 г. в России уже функционировало более 800 федеральных государственных информационных систем, обеспечивающих обмен данными между государственными органами в различных областях общественной жизни. Эти системы охватывают широкий спектр информации, включая статистические данные, а также сведения о здравоохранении, образовании и других ключевых секторах. В этом контексте использование данных из ГИС для создания лингвистических корпусов представляется особенно перспективным направлением. Несмотря на различия в уровне разработки этих систем, можно ожидать, что собранные в них данные будут обладать необходимыми качественными характеристиками, а их многообразие способно обеспечить необходимые репрезентативность и объем (Ilin, 2024). Тем не менее, учитывая риски, связанные с правовыми ограничениями на использование данных, повторное использование должно осуществляться в соответствии с едиными принципами и нормами регулирования. Эти нормы должны включать законодательные стандарты и механизмы контроля, учитывающие специфику каждого типа данных и соответствие целям их первоначального сбора.

Другим возможным решением проблемы доступа и нехватки языковых данных является использование высших учебных заведений для создания и последующего распространения лингвистических корпусов. Участие университетов в цифровизации языка может быть также оправдано и с учетом социальной значимости данного процесса. В качестве примеров успешного сотрудничества между коммерческими организациями и высшими учебными заведениями в области обработки естественного языка можно отметить совместную академическую программу Группы компаний «Центр речевых технологий» с Национальным исследовательским университетом ИТМО (Ilin & Dedova, 2019).

Вместе с тем, хотя это и решает проблему создания лингвистических корпусов, вопрос их дальнейшего распространения остается открытым. Например, университет может по различным причинам не проявлять интерес к дальнейшему распространению лингвистического корпуса или не иметь для этого необходимых ресурсов

---

10 Конституция Российской Федерации. Ст. 19. https://clck.ru/3GPBg6

11 Конституция Российской Федерации. Ст. 23. https://clck.ru/3GPBhb

12 ЦПУР. (2020). Оценка открытости государственных информационных систем в России: аналитический доклад. https://clck.ru/3GPBjT

и, соответственно, не заниматься его распространением. Вызывает также вопросы и возможность университетам, работающим по концепции предпринимательского университета и коммерциализирующим свои результаты, например через спин-офф компании, полагаться на доктрину свободного использования произведений[13] при обработке языковых данных. Все эти вопросы требуют дальнейшего тщательного анализа как с правовой, так и с других точек зрения.

2. Языковая дискриминация как форма цифрового неравенства

Поскольку применительно к разработке больших языковых моделей цифровое неравенство приводит к неравному доступу отдельных людей или социальных групп к технологиям обработки естественного языка (NLP) – невозможности в полной мере использовать данную технологию на своем языке, – проблему цифрового неравенства в первую очередь следует рассматривать в контексте языковой дискриминации.

Сама по себе проблема дискриминации со стороны систем искусственного интеллекта, хотя и не является новой, но остается актуальной и на сегодняшний день. Развитие и активное внедрение искусственного интеллекта в различные области жизни открывает новые направления для обсуждения данной проблемы, например проявления дискриминации системами искусственного интеллекта в области трудовых отношений (Morin, 2024), влияние метода профилирования[14] на человеческое достоинство (Orwat, 2024), потенциальное влияние искусственного интеллекта на дискриминацию по признаку этнической принадлежности, религии и пола (Ozkul, 2024) и т. д.

Кроме того, с увеличением автономности искусственного интеллекта и развитием генеративных моделей дискриминация начинает приобретать неявный характер, что позволяет разделять проявление дискриминации на прямую и косвенную. Например, в отличие от явных случаев дискриминации, наблюдаемых в системах предсказательной аналитики преступности, таких как алгоритмы «ПредПол» (англ. PredPol)[15] и «КОМПАС» (англ. COMPAS)[16], проявления дискриминации в генеративных системах

---

13 Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ. Ст. 1274. https://clck.ru/3GPBnL

14 Профилирование представляет собой метод интеллектуального анализа данных, который может быть автоматизированным или полуавтоматизированным и направлен на создание классов или категорий характеристик из больших наборов данных. В этом процессе данные собираются, анализируются с помощью различных алгоритмов, таких как машинное обучение, и используются для создания профилей, описывающих типичные характеристики или поведенческие модели групп или индивидов. Подробнее см. (Bosco et al., 2015).

15 PredPol (Predictive Policing) – это система предсказательной полицейской аналитики, разработанная для прогнозирования преступлений. Основная цель PredPol заключается в использовании исторических данных о преступлениях для создания карт «горячих точек» – районов, где, вероятнее всего, произойдут преступления в будущем. Подробнее см. (Browning & Arrigo, 2021).

16 COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) – это система предсказательной аналитики, предназначенная для оценки риска рецидива среди осужденных. Основная цель COMPAS заключается в анализе данных о правонарушениях, поведении и социальной истории подозреваемых с целью прогнозирования вероятности их повторного совершения преступлений. Система используется в судебной практике для помощи в принятии решений о назначении наказаний и условиях освобождения. Подробнее см. (Engel et al., 2024).

искусственного интеллекта могут быть менее очевидными. Эти системы могут, например, преимущественно создавать образы белых мужчин в ответ на повторяющиеся запросы о примерах людей, занятных на важных профессиях, что потенциально будет приводить к кумулятивным дискриминационным эффектам (Hacker et al., 2024). В таких случаях обнаружение дискриминации становится сложным, так как она может не иметь явного или очевидного характера, но тем не менее оказывает значительное влияние на представление и восприятие различных групп в обществе.

Национальная стратегия развития искусственного интеллекта на период до 2030 г.[17] (далее – Стратегия) подчеркивает, что защита прав и свобод человека является одним из основных принципов развития и использования технологии искусственного интеллекта[18], а «недискриминация» выделена в качестве одного из основных принципов развития нормативно-правового регулирования общественных отношений, связанных с развитием и использованием технологий искусственного интеллекта[19].

Статья 2 Всеобщей декларации прав человека (1948)[20] устанавливает запрет на дискриминацию, в том числе по языковому признаку. Аналогичное положение содержится и в ст. 1 (3) Устава ООН[21], а также находит свое отражение в п. 2 ст. 19 Конституции РФ, согласно которому государство гарантирует равенство прав и свобод человека и гражданина независимо от языка.

В области языковой дискриминации выявляются несколько ключевых аспектов, связанных с ее признанием, правовой защитой и общественным восприятием. Одной из основных проблем является недостаточная признанность языковой дискриминации на международном уровне. Например, дискриминация по признаку голоса часто остается незамеченной (Baugh, 2023), что может оказаться критичным при взаимодействии с технологией распознавания речи и голоса и связанных с ними цифровых продуктов: систем интерактивного ответа и голосовых помощников.

Комитет ООН[22] по правам человека неоднократно рассматривал проблему языковой дискриминации, однако его судебная практика недостаточно развита и не обеспечивает надежной защиты языковых меньшинств (Möller, 2011).

---

17 Национальная стратегия развития искусственного интеллекта на период до 2030 года, утверждена Указом Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» (далее – Национальная стратегия развития искусственного интеллекта на период до 2030 года).

18 Национальная стратегия развития искусственного интеллекта на период до 2030 года. 19 (а). https://clck.ru/3Ghyfz

19 Там же. П. 51 (10) (г). https://clck.ru/3Ghyfz

20 Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948). https://clck.ru/3GPBqd

21 Устав Организации Объединенных Наций (Принят в г. Сан-Франциско 26.06.1945). https://clck.ru/3GPBsN

22 Комитет ООН по правам человека был создан на основании Международного пакта о гражданских и политических правах, который был принят Генеральной Ассамблеей ООН в 1966 г. и вступил в силу в 1976 г. Этот комитет является органом, контролирующим выполнение государствами-участниками обязательств, взятых на себя по данному пакту. Комитет рассматривает доклады государств о том, как они соблюдают права, закрепленные в пакте, а также индивидуальные жалобы о нарушении прав (если государство признало юрисдикцию Комитета по этому вопросу). Подробнее о Комитете: https://clck.ru/3GPBvJ

Нормативно-правовая база на различных уровнях также часто не учитывает все нюансы языковой дискриминации. Законодательство на международном, региональном и национальном уровнях, как правило, не предоставляет достаточной защиты прав языковых меньшинств, что приводит к пробелам в правовой защите пострадавших (Chilingaryan et al., 2020).

Дискриминация по языковому признаку может быть определена как любое неоправданное различие или ограничение, которое ослабляет или исключает возможность реализации прав, закрепленных в международных или национальных нормативных актах, на основе языковой принадлежности. Вместе с тем необходимо добавить, что государства также несут позитивные обязательства по защите и поощрению языковых прав в рамках своего обязательства соблюдать права человека[23], в связи с чем в контексте создания больших языковых моделей представляется необходимым расширить определение языковой дискриминации, включив в него действия, направленные на препятствование сохранению или развитию языков меньшинств. Если суть первой части определения заключается в том, что языковая дискриминация возникает, когда человек испытывает худшее обращение по сравнению с другими в аналогичной ситуации из-за недостаточного или полного отсутствия владения официальным языком, установленным в данном государстве или регионе, то вторая часть будет относиться к более глубокому аспекту данной проблемы – выполнению государствами своих юридических обязательств по защите и продвижению языков меньшинств, установленных международными конвенциями и национальным законодательством. При этом необходимо отметить, что расширение понятия языковой дискриминации скорее будет отражать перспективу, к которой стремится судебная практика и научная дискуссия, чем текущее восприятие проблемы правоприменителями и юристами.

3. Проблема квалификации и критерии оценки языковой дискриминации

Неоднозначность в определении языковой дискриминации затрудняет правоприменение и порождает вопросы о критериях, применяемых при оценке этих ситуаций. Как было отмечено ранее, языковая дискриминация возникает, когда к людям обращаются неодинаково из-за их владения языком или акцента, что часто приводит к ограничению доступа к возможностям и правам (Миронова, 2019). Однако языковая дискриминация – это многогранная проблема, отличающаяся от других форм дискриминации, таких как расовая или религиозная, и зависящая от различных факторов. Анализ существующей практики позволяет выделить ряд ключевых факторов для определения языковой дискриминации. Во-первых, это численность носителей языка: уровень дискриминации часто определяется распространенностью языка в обществе. Например, в Камеруне англоязычное меньшинство сталкивается с системной дискриминацией из-за своей небольшой численности по сравнению с франкоязычным большинством (Donard, 2023).

---

[23] Например, обязательства, вытекающие из Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Федерального закона от 17.06.1996 № 74-ФЗ «О национально-культурной автономии».

Другим важным фактором является способность государства поддерживать многоязычие. Чем активнее государство создает условия для изучения и использования нескольких языков, тем ниже вероятность языковой дискриминации. Например, исследования показывают, что поддержка многоязычия в образовательных учреждениях способствует уменьшению уровня дискриминации на языковой основе (Page, 2023).

Также большое значение имеет использование языков меньшинств в общественной жизни. Когда эти языки не получают институциональной поддержки, их носители часто оказываются маргинализированы, что усиливает существующее социальное неравенство.

Кроме того, следует учитывать, что языковая дискриминация может пересекаться с другими формами дискриминации, такими как расовая, религиозная или этническая. В таких случаях люди подвергаются комплексным формам дискриминации, что значительно усугубляет проблему (Drożdżowicz & Peled, 2024). Для того чтобы проиллюстрировать комплексность проблемы, рассмотрим кратко некоторые из таких пересечений.

Непредоставление равного доступа к услугам на родном языке может нарушить право на равенство, создавая барьеры, которые мешают полноценному участию в жизни общества[24]. Эти барьеры, например, могут влиять на право на образование[25], ограничивая доступ к образовательным ресурсам и материалам на родном языке, что может снижать качество образования и ограничивать образовательные возможности.

Кроме того, языковая дискриминация затрагивает право на свободу выражения[26]. Люди должны иметь возможность свободно выражать свои мнения на языке, который они предпочитают, и ограничения в этом могут рассматриваться как нарушение этого основополагающего права. Языковая дискриминация также влияет на культурные права, так как язык является ключевым элементом культурной идентичности и самовыражения. Ограничение использования языка меньшинств в культурных и общественных контекстах может подорвать культурные права этих сообществ и их возможность сохранять и развивать свою культурную идентичность.

Доступ к правосудию также может быть затруднен языковыми барьерами, так как необходимость понимания и участия в судебных разбирательствах на родном языке является критически важной для обеспечения справедливого правосудия[27]. Языковые барьеры могут препятствовать правильному пониманию обвинений, судебного процесса или правовых решений, что может привести к несправедливым результатам.

---

24 D.H. and Others v. Czech Republic: Постановление Большой Палаты Европейского Суда по правам человека от 13 ноября 2007 года (жалоба № 57325/00).

25 Communication No. 760/1997. J.G.A. Diergaardt (late Captain of the Rehoboth Baster Community) et al. v. Namibia, Views of 25 July 2000, CCPR/C/69/D/760/1997.

26 Communication No. 221/1987. Yves Cadoret and Hervé Le Bihan v. France, Views of 11 April 1991, CCPR/C/41/D/221/1987; Communication No. 219/1986. Dominique Guesdon v. France, Views of 25 July 1990, CCPR/C/39/D/219/1986.

27 Например, отказ суда предоставить обвиняемому текст обвинительного заключения в переводе на карачаевский язык привел к отмене приговора в связи с нарушениями норм уголовного и уголовно-процессуального закона органами предварительного расследования. Подробнее см. Обзор судебной практики Верховного Суда РФ «Обзор кассационной практики Судебной коллегии по уголовным делам Верховного Суда Российской Федерации за 2003 год». (2004). Бюллетень Верховного Суда РФ, 9.

Таким образом, несмотря на возможность выделить факторы для оценки языковой дискриминации, правовая квалификация таких случаев в контексте цифровых технологий вызывает определенные трудности. Например, необходимо выяснить, можно ли считать ошибки в работе языковой модели проявлением дискриминации. Такие ошибки часто трудно обнаружить, поскольку проявление дискриминации может быть скрытым, что делает ее менее очевидной в процессе анализа. Дискриминация в моделях может быть следствием алгоритмической или человеческой предвзятости. Алгоритмическая возникает из-за ограничений или искажений в данных, на которых обучается модель, тогда как человеческое предвзятое отношение может проявиться в процессе разработки и настройки алгоритмов (Харитонова и др., 2021). Обе формы предвзятости могут не только влиять на точность и справедливость решений, но и поддерживать или усугублять существующие социальные неравенства, что в конечном счете может привести к дискриминации. Разграничение между ошибками и дискриминацией требует глубокого анализа, поскольку ошибки могут быть случайными, а могут быть результатом системных предвзятостей. Важным является понимание того, как предвзятость, и алгоритмическая, и человеческая, влияет на процесс принятия решений и насколько она интегрирована в алгоритмы и модели. Это понимание необходимо для разработки более справедливых и инклюзивных цифровых систем.

Заключение

Цель настоящей статьи заключалась в анализе конституционно-правовых аспектов создания больших языковых моделей в контексте цифрового неравенства и языковой дискриминации. В ходе исследования было установлено, что цифровое неравенство в контексте больших языковых моделей обусловлено неравномерным уровнем цифровизации языков и проявляется в ограниченном доступе к технологиям обработки естественного языка. Такой неравный доступ может негативно повлиять на реализацию конституционно гарантированных прав и требует рассмотрения через призму концепций «равенства» и запрета на дискриминацию. В свою очередь, выявление и правовая квалификация языковой дискриминации в процессе создания больших языковых моделей представляют собой сложную задачу, поскольку предвзятости в моделях могут проявляться на скрытом уровне и обладать кумулятивным дискриминационным эффектом. Дискриминация может быть вызвана как алгоритмической, так и человеческой предвзятостью. Алгоритмическая предвзятость возникает из-за ограничений или искажений в данных, на которых обучается модель, в то время как человеческая предвзятость может проявиться в процессе разработки и настройки алгоритмов. Разграничение этих категорий и оценка их влияния на процесс принятия решений становятся важными направлениями для будущих исследований, направленных на разработку механизмов, обеспечивающих равный доступ к цифровым технологиям и защиту языковых прав.

Список литературы

Миронова, М. В. (2019). Становление термина «языковая дискриминация» в современной социолингвистике. В сб. *New Language. New World. New Thinking: сборник материалов II Ежегодной международной научно-практической конференции* (с. 555–558). Москва: Дипломатическая академия Министерства иностранных дел Российской Федерации. https://elibrary.ru/bjegvs

Мушаков, В. Е. (2022). Конституционные права человека в контексте проблемы преодоления цифрового разрыва. *Вестник Санкт-Петербургского университета МВД России*, *1*(93), 69–73. EDN: https://elibrary.ru/elrbud. DOI: https://doi.org/10.35750/2071-8284-2022-1-69-73

Талапина, Э. В. (2022). Обработка данных при помощи искусственного интеллекта и риски дискриминации. Право. *Журнал Высшей школы экономики*, *1*, 4–27. EDN: https://elibrary.ru/pwepsj. DOI: https://doi.org/10.17323/2072-8166.2022.1.4.27

Харитонова, Ю. С., Савина, В. С., Паньини, Ф. (2021). Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права. *Вестник Пермского университета. Юридические науки*, *53*, 488–515. EDN: https://elibrary.ru/eukcpy. DOI: https://doi.org/10.17072/1995-4190-2021-53-488-515

Alarcón, A. A. (2022). The economics of language. In Miquel Àngel Pradilla Cardona (Ed.), *Catalan Sociolinguistics: State of the art and future challenges* (pp. 173–182). https://doi.org/10.1075/ivitra.32.12ala

Baugh, J. (2023). Linguistic profiling across international geopolitical landscapes. *Daedalus*, *152*(3), 167–177. https://doi.org/10.1162/daed_a_02024

Bosco, F., Creemers, N., Ferraris, V., Guagnin, D., & Koops, B. J. (2015). Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities. In S. Gutwirth, R. Leenes, P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20, pp. 3–33). https://doi.org/10.1007/978-94-017-9385-8_1

Browning, M., & Arrigo, B. (2021). Stop and risk: Policing, data, and the digital age of discrimination. *American Journal of Criminal Justice*, *46*(2), 298–316. https://doi.org/10.1007/s12103-020-09557-x

Chasalow, K., & Levy, K. (2021). Representativeness in statistics, politics, and machine learning. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 77–89). https://doi.org/10.1145/3442188.3445872

Chilingaryan, K., Meshkova, I., & Sheremetieva, O. (2020). International legal protection of linguistic minorities. *International Journal of Psychosocial Rehabilitation*, *24*(6), 9750–9758. EDN: https://elibrary.ru/dgcwtx. DOI: https://doi.org/10.37200/IJPR/V24I6/PR26097

Dash, N. S., & Arulmozi, S. (2018). *History, features, and typology of language corpora*. Springer Singapore. https://doi.org/10.1007/978-981-10-7458-5

Devlin, J., Chang, Ming-Wei, Lee, Kenton, & Toutanova, K. (2018). *Bert: Pre-training of deep bidirectional transformers for language understanding*. arXiv preprint arXiv:1810.04805.

Doğruöz, A. S., Sitaram, S., & Yong, Z. X. (2023). *Representativeness as a forgotten lesson for multilingual and code-switched data collection and preparation*. arXiv preprint arXiv:2310.20470 (pp. 5751–5767).

Donard, K. (2023). Legal protection of linguistic minority under discrimination: the case of anglophone Cameroon. *International Journal of Business and Technology*, *11*(2), Article 1.

Drożdżowicz, A., & Peled, Y. (2024). The complexities of linguistic discrimination. *Philosophical Psychology*, *37*(6), 1459–1482. https://doi.org/10.1080/09515089.2024.2307993

Engel, C., Linhardt, L., & Schubert, M. (2024). Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism. In *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-024-09389-8

Glauner, P. (2024). Technical foundations of generative AI models. In *Legal Tech-Zeitschrift für die digitale Anwendung*, *1*, 24–34.

Hacker, P. A (2021). Legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, *13*(2), 257–301. https://doi.org/10.1080/17579961.2021.1977219

Hacker, P., Mittelstadt, B., Zuiderveen Borgesius, F., Wachteret, S. (2024). *Generative Discrimination: What Happens When Generative AI Exhibits Bias, and What Can Be Done About It*. arXiv preprint arXiv:2407.10329. https://doi.org/10.2139/ssrn.4877398

Ilin, I. (2022). Legal Regime of the Language Resources in the Context of the European Language Technology Development. In Z. Vetulani, P. Paroubek, M. Kubis (Eds.), *Human Language Technology. Challenges for Computer Science and Linguistics. LTC 2019. Lecture Notes in Computer Science* (vol. 13212, pp. 367–376). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-05328-3_24

Ilin, I., & Dedova, M. (2019). Academic Entrepreneurship in the Field of Language Resource Creation and Dissemination. In A. Riviezzo, M. Rosaria Napolitano, & A. Garofano (Eds.), *The ESU 2019 Conference and Doctoral Programme, Naples (Italy), 8–14 September 2019. Electronic Conference Proceedings* (pp. 193–200).

Ilin, I., & Kelli, A. (2024). Natural Language, Legal Hurdles: Navigating the Complexities in Natural Language Processing Development and Application. *Journal of the University of Latvia. Law*, *17*, 44–67. https://doi.org/10.22364/jull.17.03

Ilin, I., & Kelli, A. (2019). The use of human voice and speech in language technologies: the EU and Russian intellectual property law perspectives. *Juridical International*, *28*, 17–27. https://doi.org/10.12697/ji.2019.28.03

Ilin, I. (2020). The Voice and Speech Processing within Language Technology Applications: Perspective of the Russian Data Protection Law. *Legal Issues in the Digital Age*, *1*, 99–123. EDN: https://elibrary.ru/axbzzq. DOI: https://doi.org/10.17323/2713-2749.2020.1.99.123

Ilin, I. (2024). Progress in Natural Language Processing Technologies: Regulating Quality and Accessibility of Training Data. *Legal Issues in the Digital Age*, *2*, 36–56. EDN: https://elibrary.ru/azkzba. DOI: https://doi.org/10.17323/2713-2749.2024.2.36.56

Jiang, X., Yan, L., Vavekanand, R., & Hu, M. (2023). Large Language Models in Healthcare Current Development and Future Directions. *Generative AI Research*, *2*, 12. https://doi.org/10.20944/preprints202407.0923.v1

Kelli, A., Vider, K., Pisuke, H., & Siil, T. (2016). Constitutional values as a basis for the limitation of copyright within the context of digitalisation of the Estonian language. In *Constitutional Values in Contemporary Legal Space* (Vol. II, pp. 126–139).

Li, X., Dou, Zh., Zhou, Yu., & Liu, F. (2024). CorpusLM: Towards a unified language model on corpus for knowledge-intensive tasks. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 26–37). https://doi.org/10.1145/3626772.3657778

Möller, J. T. (2011). Case Law of the UN Human Rights Committee relevant to Members of Minorities and Peoples in the Arctic Region. *The Yearbook of Polar Law Online*, *3*(1), 27–56. https://doi.org/10.1163/22116427-91000054

Monteith, B., & Sung, M. (2023). Unleashing the Economic Potential of Large Language Models: The Case of Chinese Language Efficiency. *TechRxiv*. *June 07*. https://doi.org/10.36227/techrxiv.23291831.v1

Morin, S. L. (2024). AI Discrimination in Hiring. In D. Norman (Ed.), *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 64–74). IGI Global. https://doi.org/10.4018/979-8-3693-1906-2.ch004

Orwat, C. (2024). Algorithmic Discrimination From the Perspective of Human Dignity. *Social Inclusion*, *12*, 1–18. https://doi.org/10.17645/si.7160

Ozkul, D. (2024). Artificial Intelligence and Ethnic, Religious, and Gender-Based Discrimination. *Social Inclusion*, *12*, 1–3. https://doi.org/10.17645/si.8942

Page, C. (2023). Academic language development and linguistic discrimination: Perspectives from internationally educated students. *Comparative and International Education*, *52*(2), 39–53. https://doi.org/10.5206/cie-eci.v52i2.15000

Rogers, S. E. (2016). Bridging the 21st century digital divide. *TechTrends*, *60*(3), 197–199. https://doi.org/10.1007/s11528-016-0057-0

Sohail, A., & Zhang, L. (2024). *Integrating large language models into the psychological sciences*. https://doi.org/10.1007/s12144-025-07438-2

Solovyev, V. D., & Akhtyamova, S. (2019). Linguistic Big Data: Problem of Purity and Representativeness. In *21st International Conference on Data analytics and management in data intensive domains, DAMDID/RCDL 2019* (pp. 193–204). EDN: https://elibrary.ru/tqmgbu

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*. https://doi.org/10.48550/arXiv.1706.03762

Yenduri, G., Ramalingam, M., Chemmalar Selvi, G., Supriya, Y., Srivastava, G., Maddikunta, P. K. R. et al. (2023). Generative pre-trained transformer: A comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions. In *IEEE Access* (Vol. 12, pp. 54608–54649). https://doi.org/10.1109/access.2024.3389497

Сведения об авторе

Ильин Илья Геннадьевич – магистр права в области информационных технологий, аспирант юридического факультета, Санкт-Петербургский государственный университет
Адрес: 199106, Россия, г. Санкт-Петербург, 22-я линия В.О., 7
E-mail: i.g.ilin@spbu.ru
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57765898000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/FDF-0979-2022
Google Scholar ID: https://scholar.google.com/citations?user=YruuMK0AAAAJ
РИНЦ Author ID: https://elibrary.ru/author_profile.asp?authorid=1253542

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: 10.15 / Конституционное (государственное) право
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 15 ноября 2024 г.
Дата одобрения после рецензирования – 25 ноября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:177.5:316.647.82:004.8:004.652
EDN: https://elibrary.ru/mbwjxf
DOI: https://doi.org/10.21202/jdtl.2025.4

Constitutional-Legal Aspect of Creating Large Language Models: the Problem of Digital Inequality and Linguistic Discrimination

Ilya G. Ilin

Saint Petersburg State University, Saint Petersburg, Russia

Keywords

artificial intelligence,
constitutional rights,
digital inequality,
digital technologies,
generative artificial intelligence,
human rights,
large language models,
law,
linguistic discrimination,
natural language processing

Abstract

Objective: to study the impact of digital inequality on the implementation of constitutional human rights; to identify the risks of linguistic discrimination associated with the development and use of large language models.

Methods: formal-legal and comparative-legal methods, as well as the method of theoretical modeling. These approaches are complemented by general scientific methods of cognition, allowing for a comprehensive analysis of the legal, technological and social aspects of the issue.

Results: the research found that, in relation to large language models, digital inequality arises due to the uneven digitalization of languages and manifests itself in limited access to natural language processing technology. In turn, unequal access to this technology can negatively affect the implementation of constitutionally guaranteed rights and can be viewed from the viewpoint of equality and non-discrimination concepts. The author emphasizes that unequal access to natural language processing technologies can exacerbate existing social and economic inequalities and create new forms of discrimination.

Scientific novelty: hidden and indirect forms of discrimination are analyzed that manifest themselves in artificial intelligence systems, especially in generative models. While direct forms of discrimination can be detected in predictive algorithms, generative models create more subtle but no less significant cumulative effects. These effects contribute to the formation of social stereotypes and inequalities in areas such as professional activity, gender and ethnicity. The author also draws attention to the fact that with the increasing autonomy of artificial intelligence, traditional approaches

to discrimination detection are becoming less effective, which requires the development of new analysis and regulation methods.

Practical significance: the results provide a basis for identifying and assessing the legal risks associated with unequal access to digital products using natural language processing. This contributes to the improvement of legal regulation in the field of the development and use of artificial intelligence technologies. The article offers recommendations for lawmakers, regulators, and technology developers aimed at minimizing the risks of digital inequality and linguistic discrimination.

For citation

Ilin, I. G. (2025).Constitutional-Legal Aspect of Creating Large Language Models: the Problem of Digital Inequality and Linguistic Discrimination. *Journal of Digital Technologies and Law, 3*(1), 89–107. https://doi.org/10.21202/jdtl.2025.4

References

Alarcón, A. A. (2022). The economics of language. In Miquel Àngel Pradilla Cardona (Ed.), *Catalan Sociolinguistics: State of the art and future challenges* (pp. 173–182). https://doi.org/10.1075/ivitra.32.12ala

Baugh, J. (2023). Linguistic profiling across international geopolitical landscapes. *Daedalus*, *152*(3), 167–177. https://doi.org/10.1162/daed_a_02024

Bosco, F., Creemers, N., Ferraris, V., Guagnin, D., & Koops, B. J. (2015). Profiling technologies and fundamental rights and values: regulatory challenges and perspectives from European Data Protection Authorities. In S. Gutwirth, R. Leenes, P. de Hert (Eds.), *Reforming European data protection law* (Vol. 20, pp. 3–33). https://doi.org/10.1007/978-94-017-9385-8_1

Browning, M., & Arrigo, B. (2021). Stop and risk: Policing, data, and the digital age of discrimination. *American Journal of Criminal Justice*, *46*(2), 298–316. https://doi.org/10.1007/s12103-020-09557-x

Chasalow, K., & Levy, K. (2021). Representativeness in statistics, politics, and machine learning. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 77–89). https://doi.org/10.1145/3442188.3445872

Chilingaryan, K., Meshkova, I., & Sheremetieva, O. (2020). International legal protection of linguistic minorities. *International Journal of Psychosocial Rehabilitation*, *24*(6), 9750–9758. https://doi.org/10.37200/IJPR/V24I6/PR26097

Dash, N. S., & Arulmozi, S. (2018). *History, features, and typology of language corpora*. Springer Singapore. https://doi.org/10.1007/978-981-10-7458-5

Devlin, J., Chang, Ming-Wei, Lee, Kenton, & Toutanova, K. (2018). *Bert: Pre-training of deep bidirectional transformers for language understanding*. arXiv preprint arXiv:1810.04805.

Doğruöz, A. S., Sitaram, S., & Yong, Z. X. (2023). *Representativeness as a forgotten lesson for multilingual and code-switched data collection and preparation*. arXiv preprint arXiv:2310.20470 (pp. 5751–5767).

Donard, K. (2023). Legal protection of linguistic minority under discrimination: the case of anglophone Cameroon. *International Journal of Business and Technology*, *11*(2), Article 1.

Drożdżowicz, A., & Peled, Y. (2024). The complexities of linguistic discrimination. *Philosophical Psychology*, *37*(6), 1459–1482. https://doi.org/10.1080/09515089.2024.2307993

Engel, C., Linhardt, L., & Schubert, M. (2024). Code is law: how COMPAS affects the way the judiciary handles the risk of recidivism. In *Artificial Intelligence and Law*. https://doi.org/10.1007/s10506-024-09389-8

Glauner, P. (2024). Technical foundations of generative AI models. In *Legal Tech – Zeitschrift für die digitale Anwendung*, *1*, 24–34.

Hacker, P. A (2021). Legal framework for AI training data—from first principles to the Artificial Intelligence Act. *Law, Innovation and Technology*, *13*(2), 257–301. https://doi.org/10.1080/17579961.2021.1977219

Hacker, P., Mittelstadt, B., Zuiderveen Borgesius, F., Wachteret, S. (2024). *Generative Discrimination: What Happens When Generative AI Exhibits Bias, and What Can Be Done About It*. arXiv preprint arXiv:2407.10329. https://doi.org/10.2139/ssrn.4877398

Ilin, I. (2020). The Voice and Speech Processing within Language Technology Applications: Perspective of the Russian Data Protection Law. *Legal Issues in the Digital Age*, *1*, 99–123. https://doi.org/10.17323/2713-2749.2020.1.99.123

Ilin, I. (2022). Legal Regime of the Language Resources in the Context of the European Language Technology Development. In Z. Vetulani, P. Paroubek, M. Kubis (Eds.), *Human Language Technology. Challenges for Computer Science and Linguistics. LTC 2019. Lecture Notes in Computer Science* (vol. 13212, pp. 367–376). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-05328-3_24

Ilin, I. (2024). Progress in Natural Language Processing Technologies: Regulating Quality and Accessibility of Training Data. *Legal Issues in the Digital Age*, *2*, 36–56. https://doi.org/10.17323/2713-2749.2024.2.36.56

Ilin, I., & Dedova, M. (2019). Academic Entrepreneurship in the Field of Language Resource Creation and Dissemination. In A. Riviezzo, M. Rosaria Napolitano, & A. Garofano (Eds.), *The ESU 2019 Conference and Doctoral Programme, Naples (Italy), 8–14 September 2019. Electronic Conference Proceedings* (pp. 193–200).

Ilin, I., & Kelli, A. (2019). The use of human voice and speech in language technologies: the EU and Russian intellectual property law perspectives. *Juridical International*, *28*, 17–27. https://doi.org/10.12697/ji.2019.28.03

Ilin, I., & Kelli, A. (2024). Natural Language, Legal Hurdles: Navigating the Complexities in Natural Language Processing Development and Application. *Journal of the University of Latvia*. *Law*, *17*, 44–67. https://doi.org/10.22364/jull.17.03

Jiang, X., Yan, L., Vavekanand, R., & Hu, M. (2023). Large Language Models in Healthcare Current Development and Future Directions. *Generative AI Research*, *2*, 12. https://doi.org/10.20944/preprints202407.0923.v1

Kelli, A., Vider, K., Pisuke, H., & Siil, T. (2016). Constitutional values as a basis for the limitation of copyright within the context of digitalisation of the Estonian language. In *Constitutional Values in Contemporary Legal Space* (Vol. II, pp. 126–139).

Kharitonova, Yu. S., Savina, V. S., & Pagnini, F. (2021). Artificial Intelligence's Algorithmic Bias: Ethical and Legal Issues. Perm University Herald. *Juridical Sciences*, *53*, 488–515. (In Russ.). https://doi.org/10.17072/1995-4190-2021-53-488-515

Li, X., Dou, Zh., Zhou, Yu., & Liu, F. (2024). CorpusLM: Towards a unified language model on corpus for knowledge-intensive tasks. In *Proceedings of the 47th International ACM SIGIR Conference on Research and Development in Information Retrieval* (pp. 26–37). https://doi.org/10.1145/3626772.3657778

Mironova, M. V. (2019). Formation of the term "Linguistic discrimination" in modern sociolinguistics. In *New Language. New World. New Thinking: collection of works of the 2nd Annual international scientific-practical conference* (pp. 555–558). Moscow: Diplomatic Academy of Ministry of Foreign Affairs of the Russian Federation. (In Russ.).

Möller, J. T. (2011). Case Law of the UN Human Rights Committee relevant to Members of Minorities and Peoples in the Arctic Region. *The Yearbook of Polar Law Online*, *3*(1), 27–56. https://doi.org/10.1163/22116427-91000054

Monteith, B., & Sung, M. (2023). Unleashing the Economic Potential of Large Language Models: The Case of Chinese Language Efficiency. *TechRxiv*. *June 07*. https://doi.org/10.36227/techrxiv.23291831.v1

Morin, S. L. (2024). AI Discrimination in Hiring. In D. Norman (Ed.), *Innovations, Securities, and Case Studies Across Healthcare, Business, and Technology* (pp. 64–74). IGI Global. https://doi.org/10.4018/979-8-3693-1906-2.ch004

Mushakov, V. (2022). Constitutional human rights in the context of bridging the digital divide. *Vestnik of the St. Petersburg University of the Ministry of Internal Affairs of Russia*, *2022*(1). (In Russ.). https://doi.org/10.35750/2071-8284-2022-1-69-73

Orwat, C. (2024). Algorithmic Discrimination From the Perspective of Human Dignity. *Social Inclusion*, *12*, 1–18. https://doi.org/10.17645/si.7160

Ozkul, D. (2024). Artificial Intelligence and Ethnic, Religious, and Gender-Based Discrimination. *Social Inclusion*, *12*, 1–3. https://doi.org/10.17645/si.8942

Page, C. (2023). Academic language development and linguistic discrimination: Perspectives from internationally educated students. *Comparative and International Education*, *52*(2), 39–53. https://doi.org/10.5206/cie-eci.v52i2.15000

Rogers, S. E. (2016). Bridging the 21st century digital divide. *TechTrends*, *60*(3), 197–199. https://doi.org/10.1007/s11528-016-0057-0

Sohail, A., & Zhang, L. (2024). *Integrating large language models into the psychological sciences*. https://doi.org/10.1007/s12144-025-07438-2

Solovyev, V. D., & Akhtyamova, S. (2019). Linguistic Big Data: Problem of Purity and Representativeness. In *21st International Conference on Data analytics and management in data intensive domains, DAMDID/RCDL 2019* (pp. 193–204).

Talapina, E. (2022). Artificial Intelligence Processing and Risks of Discrimination. *Law Journal of the Higher School of Economics*, *1*, 4–27. (In Russ.). https://doi.org/10.17323/2072-8166.2022.1.4.27

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, L., & Polosukhin, I. (2017). Attention is all you need. *Advances in Neural Information Processing Systems*. https://doi.org/10.48550/arXiv.1706.03762

Yenduri, G., Ramalingam, M., Chemmalar Selvi, G., Supriya, Y., Srivastava, G., Maddikunta, P. K. R. et al. (2023). Generative pre-trained transformer: A comprehensive review on enabling technologies, potential applications, emerging challenges, and future directions. In *IEEE Access* (Vol. 12, pp. 54608–54649). https://doi.org/10.1109/access.2024.3389497

Author information

Ilya G. Ilin – Master of Law (information technologies), postgraduate student, Faculty of Law, Saint Petersburg State University
Address: 22nd line of Vasilievsky Island, 7199106 Saint Petersburg, Russian Federation
E-mail: i.g.ilin@spbu.ru
ORCID ID: https://orcid.org/0000-0003-1076-2765
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57765898000
WoS Researcher ID: https://www.webofscience.com/wos/author/record/FDF-0979-2022
Google Scholar ID: https://scholar.google.com/citations?user=YruuMK0AAAAJ
RSCI Author ID: https://elibrary.ru/author_profile.asp?authorid=1253542

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 – November 15, 2024
Date of approval – November 25, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы

Бауржан Рахметов ✉

Университет КАЗГЮУ имени М. С. Нарикбаева, Астана, Казахстан

Казбек Хайзабеков

Падуанский университет, Падуя, Италия

Ключевые слова

Европейский союз, законодательство, защита данных, искусственный интеллект, конфиденциальность, поведенческая биометрия, право, правовое регулирование, распознавание лиц, цифровые технологии

Аннотация

Цель: изучение исторического развития законодательства Европейского союза в области поведенческой биометрии, выявление особенностей европейского подхода к регулированию поведенческой биометрии, а также оценка его преимуществ и недостатков.

Методы: общенаучные методы анализа и сравнения с акцентом на изучение юридических текстов, таких как директивы, регламенты и конвенции. Для обеспечения всестороннего понимания проблемы авторы также рассматривают технические аспекты поведенческой биометрии, что позволяет провести комплексный анализ как правовых норм, так и технологических процессов, лежащих в их основе.

Результаты: нормативная правовая база Европейского союза в области биометрии недостаточно четко разграничивает технологии поведенческой и физической биометрии. Это приводит к неоднозначности в понимании рисков и возможностей, связанных с использованием поведенческой биометрии. Авторы подчеркивают, что отсутствие конкретики в законодательстве создает значительные трудности для регулирующих органов, разработчиков технологий и конечных пользователей.

Научная новизна: заключается в том, что она представляет собой первое комплексное исследование исторического развития законодательства Европейского союза в области поведенческой биометрии. В статье раскрываются ключевые характеристики европейского подхода, его сильные и слабые стороны, а также проводится сравнительный анализ с опытом регулирования в Соединенных Штатах. В исследовании детально раскрываются ключевые аспекты, требующие дальнейшего законодательного урегулирования: от четкой дефиниции

✉ Контактное лицо

поведенческой биометрии до разработки комплексных механизмов обеспечения прозрачности и подотчетности при использовании данных технологий. Учитывая, что поведенческая биометрия является относительно новой и быстро развивающейся технологией, такое исследование имеет важное значение для понимания современных вызовов и перспектив ее регулирования.

Практическая значимость: определяется его многогранным характером и актуальностью для широкого круга специалистов в сфере цифровых технологий: от ученых-правоведов, правоприменителей и законодателей до разработчиков технологий искусственного интеллекта и биометрии.

Для цитирования

Рахметов, Б., Хайзабеков, К. (2025). Поведенческая биометрия в Европейском союзе: правовые вызовы и технологические перспективы. *Journal of Digital Technologies and Law*, *3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

Содержание

Введение

Регулирование поведенческой биометрии в Европейском союзе (далее – ЕС) свидетельствует о важности защиты данных и конфиденциальности в условиях быстро меняющегося технологического ландшафта. Биометрия, которая использует физические, физиологические и поведенческие характеристики для идентификации людей, привлекает все больше внимания по мере роста проблем конфиденциальности во всем мире. С момента принятия Конвенции 1981 г. о защите физических лиц в связи с автоматической обработкой персональных данных (Конвенция 108) ЕС постоянно обновляет свое законодательство в области защиты персональных данных. Ключевые документы, такие как Директива 95/46/ЕС и Общий регламент по защите данных (GDPR), помогли Европейскому союзу установить общемировой стандарт защиты персональных данных, особенно в такой чувствительной области, как биометрические данные. Недавние новшества, например, Закон ЕС об

искусственном интеллекте 2024 г. (EU AI Act), еще больше расширили сферу действия этих стандартов, в частности, в отношении использования поведенческой биометрии и искусственного интеллекта в таких чувствительных областях, как безопасность и конфиденциальность.

Несмотря на эти достижения, регулирование поведенческой биометрии сопряжено с различными трудностями, например, в том, что касается различий между физическими и поведенческими данными. Подход ЕС к регулированию биометрических данных оказал значительное влияние на законы о конфиденциальности во всем мире, однако он подвергается критике за отсутствие ясности и конкретики в определенных областях. В настоящей статье рассматривается эволюция нормативных актов ЕС по поведенческой биометрии, анализируются ключевые законодательные акты, их влияние на защиту данных и проблемы в этой области. Авторы также сравнивают подход ЕС к регулированию с подходом Соединенных Штатов, где отсутствие национального законодательства привело к менее всеобъемлющему регулированию биометрических данных.

1. Эволюция регулирования поведенческой биометрии в Европейском союзе

Чтобы получить более полное представление о том, как биометрия регулируется в ЕС, важно понимать контекст и условия, которые способствовали появлению и внедрению ее правовой базы (Carrigan & Coglianese, 2011). В связи со стремительным развитием электронной обработки данных в 1960-х и 1970-х гг. возникла острая необходимость в усилении мер по защите конфиденциальности, особенно при автоматическом сборе персональных данных. Это нашло отклик в ЕС и привело к принятию Конвенции 108 и Директивы 95/46/ЕС (De Hert, 2013). Эти документы стали первыми юридически обязательными международными нормативными актами, регулирующими защиту данных, в том числе биометрических.

Конвенция 108, подписанная 28 января 1981 г., обязала страны ЕС внести ряд конкретных изменений в свое внутреннее законодательство, руководствуясь такими принципами, как справедливый и законный сбор и автоматическая обработка данных и наличие конкретных, явных и законных целей для хранения таких данных; запрещение использовать данные в иных целях и хранить их дольше, чем необходимо. Эти принципы также включают адекватность, актуальность данных и отсутствие их избыточности. Как правило, в соответствии с положениями Конвенции 108 ответственность за управление обработкой персональных данных несут контролирующие органы[1].

В настоящее время действует обновленная версия этого документа, известная как Конвенция 108+. Статья 6 этой Конвенции предусматривает, что обработка биометрических данных для идентификации личности разрешена при условии наличия соответствующих гарантий защиты от рисков, которые угрожают интересам, правам и основным свободам человека, включая риск дискриминации. В то же время биометрические данные, используемые для однозначной идентификации, относятся к категории конфиденциальных данных, поэтому их обработка должна

[1] Convention 108 and Protocols: Background. (n.d.). Council of Europe Portal. https://clck.ru/3Ge8xN

сопровождаться определенными гарантиями. Для этого требуются: отдельное или совместное согласие субъекта данных; закон, определяющий цели, методы и конкретные условия, при которых может осуществляться обработка данных; меры конфиденциальности, основанные на анализе рисков, и меры предосторожности в области безопасности[2].

Директива 95/46/ЕС, принятая 24 октября 1995 г., также стала важным документом в области регулирования биометрии. Основное внимание было уделено защите основных прав и свобод человека при обработке данных в странах ЕС и свободному перемещению таких данных. Основная ответственность за защиту данных лежит на надзорных органах каждого отдельного государства, принявшего Директиву 95/46/ЕС. Это независимые органы, которые уполномочены давать рекомендации по административным мерам и нормативным актам, а также возбуждать судебные разбирательства в случае обнаружения нарушений требований по защите данных. Хотя в Директиве 95/46/ЕС не упоминается конкретно обработка биометрических данных, в соответствии с ее ст. 29 была создана Рабочая группа для проведения консультаций и представления мнений по вопросам функционирования и регулирования биометрических данных[3]. Так, в 2003 г. был издан «Рабочий документ по биометрии», в котором рассматривается применение положений Директивы 95/46/ЕС к биометрическим технологиям[4]. В 2012 г. Рабочая группа также опубликовала заключение по изменениям в рекомендациях, касающихся принципов и путей повышения конфиденциальности и защиты данных в биометрических приложениях[5].

Несмотря на это, на сегодняшний день Директива 95/46/ЕС считается утратившей силу в связи с ее заменой Общим регламентом по защите данных (GDPR), который положил начало новому этапу развития регулирования персональных данных. Регламент был принят в 2016 г. и вступил в силу в 2018 г. Как и Директива 95/94/ЕС, он распространяется на все страны ЕС, но не требует от них изменения своего внутреннего законодательства. Все организации как внутри ЕС, так и за его пределами должны соблюдать требования Общего регламента. Между тем Регламент требует, чтобы организации, базирующиеся за пределами ЕС и предоставляющие товары или услуги, отслеживающие поведение, обрабатывающие и хранящие данные граждан ЕС, идентифицировали своих представителей в ЕС. В свою очередь, контролеры и обработчики данных также имеют определенные обязательства. Контролеры всегда должны помнить о соблюдении мер, необходимых для эффективной защиты данных; они должны обрабатывать только те данные, которые входят в сферу их обязанностей, и не предоставлять доступ к ним никому, кроме тех, кто обязан их обрабатывать (Nguyen, 2018).

---

2 Convention 108 +. (2018). Council of Europe. https://clck.ru/3Ge94r

3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data. (1995). Official Journal of the European Union. https://clck.ru/3Ge97y

4 Working Document on Biometrics. (2003). The Working Party. https://clck.ru/3Ge9AL

5 Opinion on Developments in Biometric Technologies. (2012). The Working Party. https://clck.ru/3Ge9D4

В языке регулирующих органов термин «биометрические данные» впервые появился с введением GDPR. Статья 4 определяет биометрические данные как «персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица»[6]. Стоит отметить, что Общий регламент по защите данных предусматривает категорию специальных данных, требующих более высокого уровня защиты, которая включает и биометрические данные. В соответствии со ст. 9, обработка биометрических данных, целью которой является определение личности, состояния здоровья, сексуальной жизни и ориентации, строго запрещена, за исключением определенных условий. Например, явно выраженное согласие субъекта персональных данных позволяет обойти этот запрет[7] (Meden et al., 2021).

Наконец, Закон ЕС об искусственном интеллекте, принятый в марте 2024 г., является на сегодняшний день самым последним и актуальным нормативным актом, который также применяется к биометрии. В настоящее время искусственный интеллект оказывает огромное влияние на развитие биометрических технологий. В сочетании с биометрией системы искусственного интеллекта способствуют снижению количества человеческих ошибок и ускорению принятия решений (Rawat et al., 2023). Таким образом, Закон ЕС об искусственном интеллекте включает в себя несколько ключевых положений, направленных на регулирование биометрии, включая поведенческую биометрию. Отметим, что этот документ охватывает следующие аспекты, связанные с биометрией: биометрические данные; системы распознавания эмоций, биометрической категоризации, удаленной биометрической идентификации, удаленной биометрической идентификации в режиме реального времени и более удаленной биометрической идентификации[8]. Среди них к поведенческой биометрии относятся системы распознавания эмоций и удаленной биометрической идентификации в режиме реального времени (Xefteris et al., 2016; Alsaadi, 2021; Revett, 2008). Система распознавания эмоций предназначена для обработки таких характеристик, как направление взгляда, настроение, мимика и выражение лица, походка и сердцебиение. В связи с этим Закон ЕС об искусственном интеллекте вводит запрет на использование технологий распознавания эмоций на рабочем месте и в школах, на предиктивную полицейскую деятельность, если она основана на профилировании человека и оценке личностных характеристик, а также на ИИ, который предполагает манипулирование поведением людей или их уязвимостями. Что касается систем удаленной биометрической идентификации в режиме реального времени, то эта технология может быть использована при соблюдении строгих мер предосторожности и ограничений[9].

---

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). (2016). Official Journal of the European Union. https://clck.ru/3Ge9Gn

8 Santalu, N. (2023). Biometrics Under the EU AI Act. The International Association of Privacy Professionals. https://clck.ru/3Ge9Jz

9 Holistic AI Team. (2024). Prohibited AI Practices Under the EU AI Act. https://clck.ru/3Ge9Lf

2. Специфика регулирования поведенческой биометрии в Европейском союзе

2.1. Особенности подхода Европейского союза к регулированию поведенческой биометрии

Подход, который характеризует регулирование биометрии в ЕС, можно рассматривать как рискориентированный. Законодательство в области поведенческой биометрии сопровождается жесткими ограничительными мерами, направленными на защиту частной жизни и гражданских свобод, а также на борьбу с предвзятостью и дискриминирующими технологиями. Сбор, обработка и хранение поведенческих данных сопровождаются более высоким уровнем риска, особенно по сравнению с другими типами персональных данных (Rezaee, 2025). Дело в том, что точность анализа таких данных не позволяет полностью определить личность человека, а лишь выявляет специфические закономерности, связанные с его характером и привычками. Важно учитывать, что такие факторы, как высокий уровень стресса или физическое состояние, не позволяют поведенческим биометрическим данным точно оценить поведение человека. В свою очередь, более точное профилирование характерного поведения требует сбора значительного объема поведенческих данных. Кроме того, поскольку сбор поведенческих данных постоянно продолжается, возникает необходимость в хранении значительных объемов такой информации, что также создает дополнительные риски для конфиденциальности данных[10] (Sharma & Elmiligi, 2022).

Поведенческая биометрия – это относительно новая технология, которая сегодня активно набирает обороты, но по-прежнему сопряжена с определенными проблемами и рисками. Чтобы смягчить их, GDPR обязывает получать согласие субъектов данных на обработку и сбор их биометрических данных, в том числе поведенческих. Ранее GDPR уже классифицировал биометрические данные как чувствительные. Однако недавно принятый Закон ЕС об ИИ расширил систему классификации, добавив такие уровни риска, как неприемлемый, высокий, ограниченный, низкий или минимальный. Чтобы определить уровень риска, важно выяснить природу и масштабы применения ИИ (Arcila, 2024). Категория неприемлемого риска, которая запрещает использование ИИ, включает такие системы ИИ, которые предполагают социальную оценку, основанную на поведении или личных качествах, и манипулирование поведением или уязвимостями людей. Использование удаленной биометрической идентификации в режиме реального времени также запрещено, за исключением случаев, когда эта технология может помочь в поиске пропавших людей, предотвращении опасных для жизни ситуаций, включая прогнозируемые теракты, и выявлении подозреваемых в совершении преступлений. Система распознавания эмоций относится к категории ограниченного риска, но ее применение запрещено в учебных заведениях и на рабочих местах, за исключением медицинских оснований и соображений безопасности[11].

---

[10] Makhani, F. (2022). Beyond Fingerprints: Exploring Behavioral Biometrics For Secure Identity Verification. VikingCloud. https://clck.ru/3Ge9SS

[11] High-Level Summary of the AI Act. (2024). Future of Life Institute. https://clck.ru/3Ge9UK

2.2. Преимущества и недостатки подхода Европейского союза к регулированию поведенческой биометрии

Одним из преимуществ подхода ЕС является то, что его опыт регулирования значительно повлиял на другие страны, которые создают и развивают свое собственное законодательство о защите данных и биометрии. В работе (Greenleaf, 2012) на основании изучения 39 неевропейских стран было показано, что в законодательстве 33 из них имеется значительное сходство с Конвенцией 108. Причина этого, в частности, заключается в том, что страны таким образом демонстрируют свое стремление присоединиться к европейскому законодательству о защите частной жизни. В целом желание присоединиться к Конвенции 108 выразили Аргентина, Кабо-Верде, Маврикий, Марокко, Мексика, Сенегал, Тунис и Уругвай[12].

Конвенция 108+, которая заменила Конвенцию 108 в 2018 г., также стала влиятельным ориентиром в мировой практике регулирования защиты данных. Помимо государств – членов ЕС, обновленный протокол подписали Великобритания (в то время являвшаяся членом ЕС), Уругвай, Кабо-Верде, Маврикий, Мексика, Сенегал и Тунис. Кроме того, Аргентина, Буркина-Фасо и Марокко также присоединились к Конвенции 108+[13]. Тем не менее именно GDPR служит основным ориентиром для регулирования защиты данных во всем мире. К 2020 г. законы, аналогичные GDPR, были приняты в таких странах, как Бразилия, Канада и Южная Корея (Chen et al., 2022). Многие африканские страны, включая Танзанию, Эсватини, Руанду, Уганду и Нигерию, ввели ряд новых правил защиты данных, основанных на тех же принципах, что и GDPR[14]. Стоит отметить, что требования GDPR относятся не только к странам, но и к организациям по всему миру. Поскольку европейское законодательство требует строгих гарантий защиты данных, организациям, деятельность которых распространяется на граждан Европы, пришлось внести существенные изменения в соответствии с GDPR (Li et al., 2019; Chen et al., 2022).

Подход ЕС к регулированию биометрии, включая поведенческую биометрию, отличается высокой степенью защиты данных и конфиденциальности. Согласно ст. 9 GDPR, биометрические данные классифицируются как конфиденциальные данные, требующие особой защиты и соблюдения требований конфиденциальности. Это означает, что, как правило, обработка таких данных разрешена только при строгом соблюдении определенных условий. Например, необходимо получить явно выраженное согласие субъекта данных – физического лица, чьи данные используются. Кроме того, GDPR предоставляет субъектам данных право изучать информацию, хранящуюся в организациях, и отзывать свое согласие на сбор данных организациями. Организации, осуществляющие сбор и обработку данных граждан Европы, обязаны выразить заинтересованность в сборе личной информации, обосновать причины обладания этой информацией и представить субъектам данных информацию о себе. В целом по требованиям GDPR организации должны ограничивать обработку данных,

12 Chart of Signatures and Ratifications of Treaty 108. (n.d.). Council of Europe. https://clck.ru/3Ge9a5

13 Baker, J. (2018). What Does the Newly Signed ‘Convention 108+’ Mean for UK Adequacy? The International Association of Privacy Professionals. https://clck.ru/3Ge9ch

14 Wu, J., & Hayward, M. (2023). International Impact of the GDPR Felt Five Years on. Pinsent Masons. https://clck.ru/3Ge9gi

а также владение и передачу данных между платформами, предоставляя соответствующие средства защиты и удаления данных по истечении установленного периода. Очевидно, что подход GDPR можно считать ориентированным на пользователя. Это положительно влияет на индивидуальную ответственность, снижает риски безопасности и способствует усилению мер по обеспечению конфиденциальности (Aseri, 2020).

За нарушение вышеуказанных правил использования биометрических данных предусмотрены суровые санкции. Как правило, существует два уровня административных штрафов за несоблюдение GDPR: 1) до 10 млн евро или 2 % от годового глобального оборота, в зависимости от того, какая из этих сумм больше; 2) до 20 млн евро или 4 % от годового оборота, в зависимости от того, какая из этих сумм больше. Размер штрафа определяется конкретными положениями GDPR. Меньшая сумма назначается, если нарушена безопасность данных, а большая – если нарушены права граждан на неприкосновенность частной жизни. Например, в соответствии с практикой применения GDPR Ирландская комиссия по защите данных в 2023 г. оштрафовала Meta[15] на 1,2 млрд евро за передачу личной информации европейских пользователей в США без надлежащих механизмов защиты данных. До этого под санкции также попали такие компании, как Amazon, TikTok, WhatsApp, Google и др.[16]

Наиболее существенными недостатками европейского подхода являются несовершенство классификации и отсутствие конкретики в некоторых аспектах. В частности, европейские регулирующие органы не учитывают тот факт, что разные типы биометрии используют разные типы данных; только поведенческая биометрия собирает такие данные, как динамика нажатия клавиш, движения мыши, ввод данных с сенсорного экрана, движения глаз, жесты и походка (Eberz et al., 2017; Cheung & Vhaduri, 2020). Вместо этого европейское законодательство содержит лишь общие толкования и руководящие принципы, касающиеся физических, психологических и поведенческих особенностей. Этот недостаток можно проследить как в прошлом, имея в виду Конвенцию 108 и Директиву 95/46/ЕС, так и в настоящее время, в Конвенции 108+, GDPR и Законе ЕС об искусственном интеллекте. Дело в том, что динамичный характер поведенческих данных, который не позволяет прогнозировать, моделировать или получать их так же легко, как физические данные, делает их неподходящими для действующих правил ЕС, которые охватывают только физическую биометрию. Компании и финансовые учреждения в ЕС, которые уже приступили к последовательному внедрению поведенческой биометрии, по-прежнему руководствуются правилами сбора физических данных[17] (Kindt, 2018).

Проблема неопределенности также очевидна в других важных положениях нормативных актов, касающихся использования биометрических данных. Например, в GDPR не проводится существенного различия между основными сравнительными функциями биометрических технологий, в частности между верификацией и идентификацией. Верификация предполагает использование

---

15 Мета – организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

16 20 Biggest GDPR Fines So Far. (2024). Data Privacy Manager. https://clck.ru/3Ge9me

17 Özal, M. (2020). 'Behavioral Biometrics': A Brief Introduction from the Perspective of Data Protection Law. CiTiP Blog. https://clck.ru/3Ge9pA

биометрических данных в соотношении «один к одному» (1 : 1), а идентификация – «один ко многим» (1 : n). Стоит отметить, что, по мнению Совета Европы и национальных органов по надзору за защитой данных, функция верификации более безопасна, чем метод идентификации, поскольку не требует использования базы данных. Напротив, использование биометрической идентификации требует обширного сбора и хранения биометрической информации в базах данных. Кроме того, следует отметить, что биометрическая идентификация сопряжена с дополнительными рисками из-за вероятностного сопоставления, что отрицательно сказывается на уровне точности. Соответственно, европейские регулирующие органы должны объективно учитывать относительные риски, связанные как с верификацией, так и с идентификацией, при введении соответствующих правил применения этих двух основных функций биометрических технологий[18].

3. Сравнительный анализ подходов к регулированию поведенческой биометрии Европейского союза и опыта Соединенных Штатов Америки

Чтобы лучше понять систему регулирования поведенческой биометрии в ЕС, будет полезно изучить опыт США и сравнить его с подходом ЕС. Наиболее примечательно, что вместо единого национального законодательства, как в ЕС, в Соединенных Штатах биометрия регулируется на уровне штатов[19].

Во многих штатах, включая Иллинойс, Техас и Арканзас, действуют различные законы, направленные на регулирование биометрии и биометрических данных. Для начала стоит отметить штат Иллинойс, который стал первым штатом, регулирующим сбор, использование и хранение биометрических данных, введя в 2008 г. Закон о конфиденциальности биометрической информации (Biometric Information Privacy Act, BIPA). Согласно этому закону, компании обязаны получать письменное согласие от субъектов данных перед сбором их биометрической информации и ограничивать такие методы, как сканирование сетчатки или радужной оболочки глаза, снятие отпечатков пальцев, образцов голоса, сканирование геометрии лица и кистей рук. Другими словами, другие биологические и поведенческие данные не считаются биометрическими идентификаторами в соответствии с этим законом (Illman, 2017). Аналогичные определения биометрических идентификаторов содержатся в Законе штата Техас от 2009 г. в разделе 503.001[20].

В штате Арканзас принят Закон о биометрических данных, который фокусируется исключительно на биологических параметрах, исключая данные о поведении. Этот нормативный акт определяет биометрические данные как информацию о биологических характеристиках человека, таких как отпечатки пальцев, изображение лица или глаз, ДНК и другие уникальные биологические особенности, используемые для идентификации[21].

---

18 Kindt, E. (2020). A First Attempt at Regulating Biometric Data in the European Union. AI Now Institute. https://clck.ru/3Ge9ti

19 Biometric Data Protection (Privacy – EU, UK and US). (2021). https://clck.ru/3Ge9w2

20 2023 Texas Statutes Business and Commerce Code. https://clck.ru/3GePrv

21 Arkansas Personal Information Protection Act. https://clck.ru/3GeRBo

Различные законы Соединенных Штатов неодинаково интерпретируют биометрические данные. Среди них Закон штата Калифорния о защите прав потребителей (California Consumer Privacy Act, далее – CCPA) от 2018 г., который значительно расширяет понимание биометрических данных. Согласно этому закону, биометрическая информация включает в себя «физиологические, биологические или поведенческие характеристики человека, включая ДНК, которые могут использоваться отдельно или в сочетании с другими данными для установления личности»[22]. Сюда входят не только традиционные биометрические идентификаторы, но и поведенческие паттерны, такие как нажатие клавиш, походка, привычки сна, данные о физических нагрузках и состоянии здоровья, которые могут идентифицировать человека[23]. Примечательно, что в соответствии с CCPA граждане штата имеют больше возможностей для контроля над своими биометрическими данными, включая права на общее раскрытие данных, на запрашивание и удаление информации, а также на «равное обслуживание и расценки» (Ghelardi, 2020).

Кроме того, Закон США о праве на неприкосновенность частной жизни от 2024 г., являющийся преемником Закона США о конфиденциальности и защите данных от 2021 г., направлен на установление четких общенациональных прав и средств защиты данных. Законопроект был внесен в Палату представителей и в Сенат в апреле 2024 г. и месяц спустя был одобрен Подкомитетом по данным, инновациям и торговле. Теперь он должен будет пройти через полный комитет и обе палаты Конгресса, прежде чем вступит в силу в качестве закона. Этот законопроект определяет биометрическую информацию как данные, полученные в результате технологической обработки уникальных биологических, физических или физиологических характеристик, включая отпечатки пальцев, изображение лица и походки и другие характеристики. Важно отметить, что законопроект был разработан по образцу GDPR, действующего в ЕС[24].

По сравнению с законодательством ЕС, американское законодательство менее проработано. Законы принимаются не на федеральном уровне, а на уровне штатов, что указывает на необходимость более комплексного подхода (Neace, 2020). Также становится очевидным, что в этих нормативных актах, как и в нормативных актах ЕС, нет четкого различия между физической и поведенческой биометрией. Хотя в некоторых законах упоминаются поведенческие характеристики, до сих пор нет четкого законодательного определения или регулирования поведенческой биометрии. Следовательно, вопросы, связанные с поведенческой биометрией, остаются недостаточно решенными и требуют дальнейшего законодательного внимания и разработки. Необходимость уделять пристальное внимание поведенческим биометрическим данным, включая такие характеристики, как движения рук и направление взгляда, была также четко сформулирована исполнительной властью в Указе президента Джо Байдена об искусственном интеллекте[25].

---

22 California Consumer Privacy Act. https://clck.ru/3GeRFp

23 What is the California Consumer Privacy Act (CCPA)? (2024). TermsFeed. https://clck.ru/3GeAJh

24 Wright, V. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. BigID. https://clck.ru/3GeALE ; Pınarbaşı, A. T. (2024). The American Privacy Rights Act (APRA): Everything You Need to Know. Didomi. https://clck.ru/3GeANc

25 Brunetti, F. (2024). Behavioral Characteristics as a Biometric: Something to Keep an Eye (Scan) on. The International Association of Privacy Professionals. https://clck.ru/3GeATg

Заключение

Подводя итог, можно сказать, что регулирование поведенческой биометрии в ЕС претерпело значительные изменения, определяемые ключевыми законодательными актами, такими как Конвенция 108, Директива 95/46/ЕС, а совсем недавно – Общим регламентом о защите данных 2018 г. и Законом ЕС об искусственном интеллекте 2024 г. Эти документы заложили прочную основу для защиты персональных данных, особенно биометрических, отнесенных к категории конфиденциальной информации. Введение определения и строгих правил обработки биометрических данных в GDPR установило глобальный стандарт, оказавший влияние не только на европейские страны, но и на правовую практику во всем мире. Однако некоторые проблемы остаются нерешенными, например, проведение различия между физической и поведенческой биометрией и решение сложных задач, связанных с такими биометрическими технологиями, как верификация и идентификация.

Сравнение подхода ЕС с подходом Соединенных Штатов свидетельствует о более всеобъемлющей и унифицированной нормативно-правовой базе ЕС, в отличие от разрозненных законов на уровне штатов в США. Несмотря на то, что США добились прогресса в принятии таких нормативных актов, как Закон штата Иллинойс о конфиденциальности биометрической информации (BIPA) и более поздний Закон о праве на неприкосновенность частной жизни, отсутствие единого национального подхода вызывает обеспокоенность. Например, проблеме поведенческой биометрии в США по-прежнему уделяется недостаточно внимания. Поскольку такие технологии, как искусственный интеллект, продолжают развиваться и их взаимосвязь с биометрическими технологиями становится все более тесной, важно подчеркнуть, что ЕС и США должны усилить свои нормативные акты для защиты персональных данных и для содействия этичному использованию биометрических данных. Однако, учитывая новизну поведенческой биометрии, необходимы также дальнейшие исследования в области правового регулирования персональных данных.

Список литературы

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

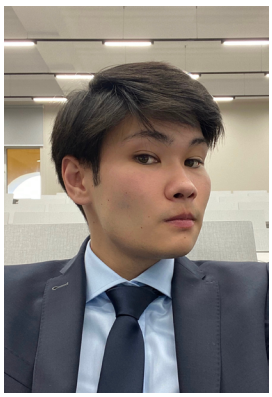
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Сведения об авторах

Рахметов Бауржан – PhD в области политологии и международных отношений, ассистент-профессор, Международная школа экономики, Университет КАЗГЮУ имени М.С. Нарикбаева
Адрес: Казахстан, 010000, г. Астана, Коргалжинское шоссе, 8
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
WoS Researcher ID: https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ



Хайзабеков Казбек – магистрант в области европеистики и глобальных исследований, кафедра политологии, права и международных исследований, Падуанский университет
Адрес: Италия, 35122, г. Падуя, ул. 8 февраля, 2
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Бауржан Рахметов является членом редакционной коллегии данного журнала; статья прошла рецензирование на общих условиях.

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 – 19 сентября 2024 г.
Дата одобрения после рецензирования – 23 октября 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:341:57.087.1:316.642.4
EDN: https://elibrary.ru/joupzt
DOI: https://doi.org/10.21202/jdtl.2025.5

Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects

Baurzhan Rakhmetov ✉
M. Narikbayev KAZGUU University, Astana, Kazakhstan

Kazbek Khaizabekov
University of Padova, Padova, Italy

Keywords

artificial intelligence,
behavioral biometrics,
data protection,
digital technologies,
European Union,
facial recognition,
law,
legal regulation,
legislation,
privacy

Abstract

Objective: to study the historical development of the European Union legislation on behavioral biometrics; to identify the features of the European approach to the regulation of behavioral biometrics, to assess its advantages and disadvantages.

Methods: general scientific methods of analysis and comparison, with an emphasis on the study of legal texts such as directives, regulations and conventions. To ensure a comprehensive understanding of the issue, the authors also consider the technical aspects of behavioral biometrics, which allows for a comprehensive analysis of both legal norms and the technological processes underlying them.

Results: the research demonstrates that the European Union regulatory legal framework on biometrics does not clearly distinguish between behavioral and physical biometrics technologies. This leads to ambiguity in understanding the risks and opportunities associated with the use of behavioral biometrics. The authors emphasize that the insufficiently specific legislation creates significant difficulties for regulators, technology developers, and end users.

Scientific novelty: the article is the first comprehensive study of the historical development of European Union legislation on behavioral biometrics. The work reveals the key characteristics of the European approach, its strengths and weaknesses, and compares it with the United States' regulatory practice. The study reveals the key aspects that require further regulation: from a clear definition of behavioral biometrics to the development of comprehensive mechanisms to ensure transparency and accountability in the use of these

✉ Corresponding author

technologies. Given that behavioral biometrics is a relatively new and rapidly developing technology, the research is important for understanding current challenges and prospects for its regulation.

Practical significance: the research is multifaceted and relevant for experts in digital technologies: legal scholars, law enforcement officers, legislators, and developers of artificial intelligence and biometrics technologies.

For citation

Rakhmetov, B., & Khaizabekov, K. (2025). Behavioral Biometrics in the European Union: Legal Challenges and Technological Prospects. *Journal of Digital Technologies and Law, 3*(1), 108–124. https://doi.org/10.21202/jdtl.2025.5

References

Alsaadi, E. (2021). *Study on Most Popular Behavioral Biometrics, Advantages, Disadvantages and Recent Applications: A Review*. https://doi.org/10.13140/RG.2.2.28802.09926

Arcila, B. B. (2024). AI liability in Europe: How does it complement risk regulation and deal with the problem of human oversight? *Computer Law & Security Review*, *54*, 106012. https://doi.org/10.1016/j.clsr.2024.106012

Aseri, A. (2020). The Implication of the European Union's General Data Protection Regulation (GDPR) on the Global Data Privacy. *Journal of Theoretical and Applied Information Technology*, *98*(4), 692–702.

Carrigan, C., & Coglianese, C. (2011). The Politics of Regulation: From New Institutionalism to New Governance. *Annual Review of Political Science*, *14*(1), 107–129. https://doi.org/10.1146/annurev.polisci.032408.171344

Chen, C., Frey, C. B., & Presidente, G. (2022). Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *Oxford Martin School*.

Cheung, W., & Vhaduri, S. (2020). Continuous Authentication of Wearable Device Users from Heart Rate, Gait, and Breathing Data. *2020 8th IEEE RAS/EMBS International Conference for Biomedical Robotics and Biomechatronics (BioRob)*, 587–592. https://doi.org/10.1109/BioRob49111.2020.9224356

De Hert, P. (2013). Biometrics and the Challenge to Human Rights in Europe. Need for Regulation and Regulatory Distinctions. In: P. Campisi (Eds.), *Security and Privacy in Biometrics* (pp. 369–413). Springer London. https://doi.org/10.1007/978-1-4471-5230-9_15

Eberz, S., Rasmussen, K. B., Lenders, V., & Martinovic, I. (2017). Evaluating Behavioral Biometrics for Continuous Authentication: Challenges and Metrics. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 386–399. https://doi.org/10.1145/3052973.3053032

Ghelardi, E.-M. (2020). Closing the Data Gap: Protecting Biometric Information Under the Biometric Information Privacy Act and the California Consumer Protection Act. *St. John's Law Review*, *94*(3).

Greenleaf, G. (2012). The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Illman, E. J. (2017). Data Privacy Laws Targeting Biometric and Geolocation Technologies. *The Business Lawyer*, *73*(1), 191–198.

Kindt, E. (2018). Having Yes, Using No? About the New Legal Regime for Biometric Data. *Computer Law & Security Review*, *34*(3), 523–538. https://doi.org/10.1016/j.clsr.2017.11.004

Li, H., Yu, L., & He, W. (2019). The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, *22*(1), 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Meden, B., Rot, P., Terhorst, P., Damer, N., Kuijper, A., Scheirer, W. J., Ross, A., Peer, P., & Struc, V. (2021). Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE Transactions on Information Forensics and Security*, *16*, 4147–4183. https://doi.org/10.1109/TIFS.2021.3096024

Neace, G. (2020). Biometric Privacy: Blending Employment Law with the Growth of Technology. *UIC Law Review*, *53*(1).

Nguyen, F. Q. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, *7*(1), 61–84.

Rawat, Y., Gupta, Y., Khothari, G., Mittal, A., & Rautela, D. (2023). The Role of Artificial Intelligence in Biometrics. *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, 622–626. https://doi.org/10.1109/ICECAA58104.2023.10212224

Revett, K. (2008). *Behavioral Biometrics: A Remote Access Approach*. Wiley.

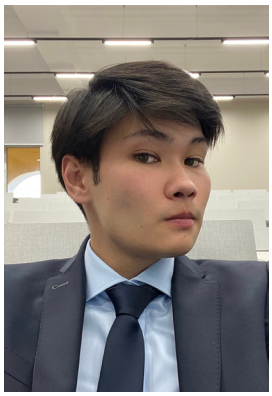
Rezaee, K. (2025). Machine Learning and Facial Recognition for Down Syndrome Detection: A Comprehensive review. *Computers in Human Behavior Reports*, *17*, 100600. https://doi.org/10.1016/j.chbr.2025.100600

Sharma, M., & Elmiligi, H. (2022). Behavioral Biometrics: Past, Present and Future. *Recent Advances in Biometrics*. IntechOpen. https://doi.org/10.5772/intechopen.102841

Xefteris, S., Doulamis, N., Andronikou, V., Varvarigou, T., & Cambourakis, G. (2016). Behavioral Biometrics in Assisted Living: A Methodology for Emotion Recognition. *Engineering, Technology & Applied Science Research*, *6*(4), 1035–1044. https://doi.org/10.48084/etasr.634

Authors information

Baurzhan Rakhmetov – PhD (Politics and International Relations), Assistant Professor, International School of Economics, M. Narikbayev KAZGUU University
Address: 8 Korgalzhyn street, 010000, Astana, Kazakhstan
E-mail: b_rakhmetov@kazguu.kz
ORCID ID: https://orcid.org/0000-0003-3948-9977
WoS Researcher ID: https://www.webofscience.com/wos/author/record/32537389
Google Scholar ID: https://scholar.google.com/citations?user=hanfRwoAAAAJ



Kazbek Khaizabekov – Master's Student, European and Global Studies, Department of Political Science, Law, and International Studies, University of Padova
Address: Via VIII Febbraio, 2, 35122 Padova PD, Italy
E-mail: khaizabekovk@gmail.com
ORCID ID: https://orcid.org/0009-0009-8241-8016
WoS Researcher ID: https://www.webofscience.com/wos/author/record/MIN-4357-2025

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

Baurzhan Rakhmetov is a member of the Editorial Board of the Journal; the article has been reviewed on general terms.

Thematic rubrics

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

Article history

Date of receipt – September 19, 2024
Date of approval – October 23, 2024
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Универсальная система управления информационной безопасностью: организационно-правовые принципы

Мусадак Ахмед Хади ✉

Технологический университет, Багдад, Ирак

Мохаммед Наджм Абдулредха

Багдадский университет, Багдад, Ирак

Ключевые слова

законодательство,
защита информации,
информационная безопасность,
информационные технологии,
кибербезопасность,
организационная структура,
право,
правовое регулирование,
управление информационной безопасностью,
цифровые технологии

Аннотация

Цель: разработка универсальных организационно-правовых принципов построения системы управления информационной безопасностью, которые позволят каждой организации создать собственную эффективную систему управления информационной безопасностью с учетом ее уникальных бизнес-целей и задач.

Методы: основаны на интеграции ключевых элементов управления информационной безопасностью, таких как видение, стратегия, цели, политики, стандарты, процессы и матрицы. Видение и цели задают направление развития организации, политики и стандарты обеспечивают концептуальную основу для защиты информации, процессы позволяют систематически достигать поставленных задач, а матрицы предоставляют инструменты для оценки и контроля всей структуры. Предложенные принципы согласуются с международными стандартами, нормативными требованиями и лучшими практиками в области информационной безопасности.

Результаты: разработанная система управления информационной безопасностью позволяет четко распределить роли и обязанности среди сотрудников организации, обеспечивая эффективное внедрение системы управления. Авторы также анализируют существующие принципы безопасности информационных технологий, интегрируя их в стратегию безопасности, которая соответствует целям организации. Предложенная универсальная система соответствует нормативным правовым требованиям и может быть адаптирована для использования в организациях любого масштаба и профиля.

✉ Контактное лицо

Научная новизна: заключается в представлении практического подхода к внедрению системы управления информационной безопасностью, основанного на опыте авторов, а также на мировых стандартах, системах контроля и правовых актах. В отличие от существующих подходов предлагаемая система является гибкой и может быть адаптирована под специфику любой организации, что делает ее универсальным инструментом для управления информационной безопасностью.

Практическая значимость: состоит в предоставлении структурированного подхода к созданию универсальной системы управления информационной безопасностью, который может быть использован организациями, испытывающими недостаток знаний и ресурсов для реализации подобных инициатив. Авторы предлагают общую структуру, которая может быть адаптирована в зависимости от активов организации, уровня подготовки сотрудников и их осведомленности в вопросах информационной безопасности. Это делает настоящую работу ценным ресурсом для специалистов, стремящихся повысить уровень защиты информации в своих организациях

Для цитирования

Хади, М. А., Абдулредха, М. Н. (2025). Универсальная система управления информационной безопасностью: организационно-правовые принципы. *Journal of Digital Technologies and Law*, *3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

Содержание

Введение

Информационная безопасность зародилась еще в древние времена, когда египтяне, греки и римляне применяли методы защиты сообщений, например, криптографию. Одним из первых и самых известных людей, защищавших сообщения, был Юлий Цезарь. Он изобрел и использовал шифр Цезаря для защиты своих личных сообщений в военных целях. С тех пор многое было сделано для решения этой проблемы, и теперь ею занимаются организации, в обязанности которых входит обеспечение информационной безопасности. В Средние века было изобретено множество методов защиты данных, например, стеганография, которая основана на сокрытии факта передачи сообщения (Rao & Nayak, 2014; Hadi et al., 2023; Wu et al., 2021).

В 1889 г. британское правительство приняло Закон о государственной тайне, заложив принципы классификации для защиты конфиденциальных данных. Кроме того,

в 1919 г. были созданы государственные кодексы безопасности. Они применялись во время Первой мировой войны для обеспечения безопасности передачи секретных данных. К этому времени было изобретено множество методов и алгоритмов защиты, таких как алгоритмы классификации, алгоритмы криптографии, алгоритмы взлома кодов (Ohki et al., 2009).

Во время Второй мировой войны немцы спроектировали и создали одно из самых важных устройств для защиты информации – «Энигма». Это электромеханическое устройство использовалось для шифрования и дешифрования сообщений о военных действиях. Математик и криптоаналитик Алан Тьюринг, работавший в Британской правительственной школе кодов и шифров, разгадал немецкий код и расшифровал его. В эту эпоху было сделано множество технологических достижений в области информационной безопасности, защиты связи, шифрования и компьютерных наук, которые облегчили обмен информацией и конфиденциальными данными (Rastogi & von Solms, 2005).

В период с 1960 по 1990 г. сфера информационной безопасности значительно продвинулась в связи с развитием цифровых электронных и информационных технологий. В этот период были изобретены первые мейнфреймовые компьютеры; системы с разделением времени получили большее значение с развитием механизмов защиты данных. Кроме того, развитие сетевых комплексов ARPANET сопровождалось разработкой стандарта шифрования данных (Data Encryption Standard, DES) на основе симметричного ключа. Затем на сцену вышли локальные сети (Local Area Networks, LAN) и персональные компьютеры (PC), а организации начали внедрять системы обнаружения вторжений (Intrusion Detection Systems, IDS), системы предотвращения вторжений (Intrusion Prevention Systems, IPS) и межсетевые экраны для защиты информации в сетях. К концу 1980-х гг. информационная безопасность стала важным аспектом компьютерных и сетевых операций, что заложило основу для эры кибербезопасности[1] (Bendovschi, 2015; Johnston & Hale, 2009).

С 1990 по 2024 г. информационная безопасность стремительно развивалась благодаря расширению концепций безопасности и средств защиты. Основной причиной этого стало изобретение Интернета в 1990-х гг., которое поставило сложные задачи в сфере информационной безопасности, например, преобразование обычных протоколов в защищенные (HTTP в HTTPS) путем добавления протоколов безопасности (SSL). Кроме того, появились новые технологии, такие как IoT, блокчейн, облачные вычисления, квантовые компьютеры и искусственный интеллект. Это породило множество векторов атак, включая кибератаки, что усложнило достижение информационной безопасности организации. В результате для обеспечения безопасности данных каждая организация должна была разработать и внедрить собственную систему управления информационной безопасностью (далее – УИБ) (Corriss, 2010; Moulton & Coles, 2003; AlGhamdi et al., 2020).

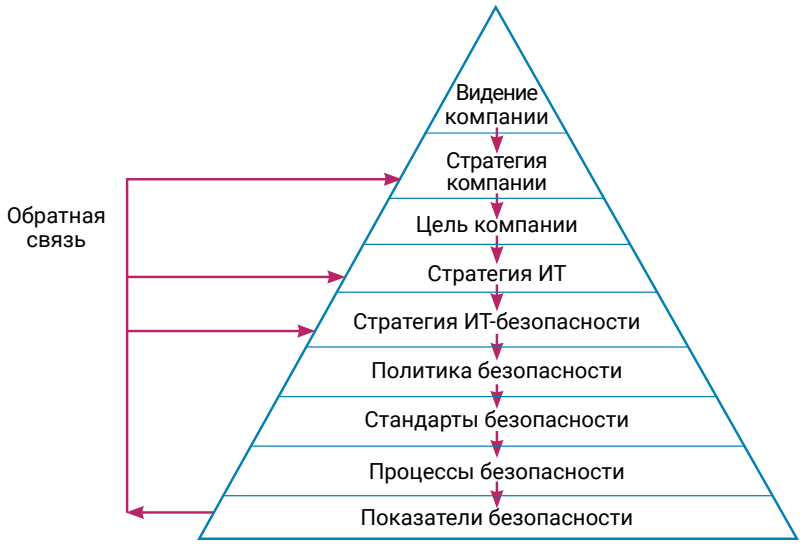
В настоящее время основным направлением деятельности в области информационной безопасности является управление всеми активами, такими как люди, риски, инциденты, уязвимости, а также планирование обеспечения непрерывности бизнеса. С другой стороны, для измерения и оценки с целью достижения эффективности программы УИБ, а также улучшения деятельности организации, используются метрики и другие инструменты мониторинга процессов и процедур. Однако информационную безопасность необходимо рассматривать как важнейшую бизнес-задачу,

[1] Gregory, P. H. (2018). CISM®: Certified Information Security Manager Exam Guide. New York: McGraw Hill Education.

поскольку отсутствие защиты данных приводит к серьезным проблемам в организациях. Это свидетельствует о недостаточности понимания и знаний у высшего руководства и советов директоров. Кроме того, государственные и частные организации сталкиваются с проблемами обеспечения информационной безопасности на уровне совета директоров из-за недостатка знаний или навыков в области кибербезопасности[2] (Carcary et al., 2016; Rocha Flores et al., 2014).

В первую очередь сотрудники, руководители и члены совета директоров должны понимать важность наличия УИБ, иначе ее невозможно будет эффективно применять. Во-вторых, для успешного внедрения УИБ должна существовать надежная программа управления сектором ИТ. Адекватная структура УИБ должна быть поддержана адекватной структурой ИТ, и они должны быть интегрированы для достижения целей и задач организации. В стратегическом плане система ИТ помогает деятельности организации, поддерживая операционную эффективность. Архитектура системы УИБ предлагает высокоорганизованный метод контроля за ИТ-процессами и активами. В конечном итоге, проще говоря, сотрудничество в управлении УИБ и IT необходимо для того, чтобы гарантировать, что информационная безопасность государственных и частных организаций не только присутствует, но и согласуется с их общими бизнес-целями (S. H. von Solms & R. von Solms, 2010).

В настоящей статье предлагается эффективная система УИБ (включая кибербезопасность) для государственных и частных организаций, которая поможет им защищать и контролировать свои активы и ИТ-сектор. Поскольку информационная безопасность подразумевает защиту всех форм информации, кибербезопасность – это одно из направлений информационной безопасности, направленное на защиту цифровой информации. Поэтому все, что применяется в рамках УИБ, обязательно включает в себя средства обеспечения кибербезопасности. Более того, предлагаемая ниже структура УИБ должна работать в соответствии с законами и правилами, что делает ее реализацию последовательной (рис.). В конечном счете управление ИТ-сектором и УИБ должно осуществляться в сотрудничестве, что упростит его и сделает более отвечающим потребностям организации.



Концептуальная структура организации
Источник: (H., von S.S. & Solms, 2010).

[2] Gregory, P. H. (2022). CISM Certified Information Security manager all-in-one exam guide. New York: McGraw Hill.

Данная работа построена следующим образом. В разделе 1 изложен ключевой вопрос о целях и задачах создания системы УИБ и ее подробное описание. В разделе 2 представлены роли и обязанности сотрудников с матрицей распределения ответственности RACI и составляющими элементами организации. В разделе 3 описаны лучшие образцы УИБ в качестве основы для разработки индивидуальной системы УИБ. В разделе 4 представлены предлагаемая структура УИБ, регулирующие законы и нормы, а также действия организации по внедрению системы УИБ.

1. Почему организации должны иметь систему управления информационной безопасностью?

В данном разделе представлены потребности, обязательно присутствующие у организаций, имеющих собственную систему УИБ. В целом УИБ необходима государственным и частным организациям в связи с быстрым развитием технологий и социальных сетей, о чем говорилось во введении. Таким образом, деятельность многих государственных организаций в различных секторах существенно зависит от их информационной и ИТ-инфраструктуры. Эта зависимость может достигнуть уровня, когда для поддержания своей деятельности организация должна будет сосредоточиться на продуктах/услугах, связанных с информацией. Организациям также необходимо будет обеспечить безопасность своих активов и данных, учитывая приоритетность их сферы деятельности и применяя принципы конфиденциальности, целостности и доступности (Confidentiality, Integrity, and Availability, CIA)[3].

Цель разработки системы УИБ – удовлетворить потребности бизнеса, включая стратегию обеспечения и эффективного контроля информационной безопасности. Кроме того, при этом устанавливаются формальные средства контроля безопасности, обеспечивающие деятельность и ее желаемые результаты. Программы секторов ИТ и безопасности структурируются и выполняются последовательно, что отвечает приоритетам бизнеса. При этом формальные средства контроля и измерения процессов дают руководству четкое представление о том, как организация управляет безопасностью. Эффективность программы УИБ обеспечивается путем согласования управления безопасностью с процедурами, которые используются в корпоративном и ИТ-управлении. Управление безопасностью должно быть интегрировано в процессы ИТ и корпоративного управления. В конечном итоге благодаря управлению безопасностью и стратегическому планированию предлагаемая система УИБ может обеспечить общее управление как в государственных, так и в частных организациях (Rebollo et al., 2015).

Итак, для эффективного внедрения системы УИБ руководители высшего звена организации должны взять на себя ответственность за защиту данных в своих организациях. Вот некоторые виды деятельности, которые должны быть включены в рамочную программу УИБ организации (Rebollo et al., 2015):

а) управление рисками: необходимо управлять рисками организации, чтобы смягчить существующие и будущие риски. Однако в некоторых случаях руководство должно пойти на компромисс и принять определенный уровень риска для поддержания функциональности организации;

[3] Gregory, P. H. (2020). CISA Certified Information Systems Auditor all-in-one exam guide. New York: McGraw-Hill.

б) соответствие: организация должна действовать в соответствии с законами и нормативными актами, действующими в стране, а также иметь собственные стандарты для защиты своих данных и активов;

в) управление реагированием на чрезвычайные ситуации: руководители организации должны разработать стратегию работы с чрезвычайными ситуациями, чтобы контролировать внезапные события, минимизировать их последствия и поддерживать возможности организации по смягчению последствий;

г) план обеспечения непрерывности бизнеса (далее – ПНБ), гарантирующий, что организация будет продолжать функционировать во время и после любой чрезвычайной ситуации или бедствия. Кроме того, он включает в себя план аварийного восстановления (далее – ПАВ) для поддержания деятельности организации;

д) план аварийного восстановления: это часть ПНБ, которая направлена на восстановление данных, инфраструктуры, ИТ-систем организации после чрезвычайной ситуации или бедствия. В ПАВ должна быть предусмотрена команда экстренной помощи, которая создает резервные копии (зеркала), различные сайты (горячий, холодный) и документацию;

е) осведомленность о безопасности: важно поддерживать определенный уровень осведомленности всех членов организации об информационной безопасности и о том, что дает система УИБ, путем проведения различных обучающих программ в течение всего года, особенно для ИТ-сектора и управленческого персонала.

Благодаря этой деятельности руководители высшего звена занимают активную позицию в управлении и руководстве информационными системами организации, обеспечивая устойчивость к потенциальным угрозам и развивая стратегический подход к управлению безопасностью.

2. Должности, роли и зоны ответственности в организации

Отдел информационной безопасности в любой организации воспринимается как «все запрещающий» и препятствующий ведению бизнеса. Такой образ сложился благодаря тому, что его руководители иногда проявляют чрезмерную осторожность в отношении рисков, ограничивают расширение организации, внедрение инновационных продуктов и услуг. В результате такая репутация порождает у персонала ИТ-сектора и других подразделений нежелание взаимодействовать со специалистами по безопасности; они опасаются, что сотрудничество может помешать их работе. Более того, признаком правильного внедрения системы УИБ служит то, что работники организации понимают свои обязанности, роли и зону ответственности и четко их придерживаются. Поэтому организациям следует установить формальные роли и обязанности, в соответствии с которыми каждый сотрудник должен получить инструкции по сохранению данных и активов организации. Эти роли должны быть связаны с названиями должностей, указывая на место сотрудника в организации. Названия должностей нужны в организациях, чтобы гарантировать, что каждый сотрудник работает в соответствии со своими должностными обязанностями. Как правило, названия должностей связаны с позицией сотрудника, которая отражает уровень его полномочий. Вот некоторые названия должностей, перечисленные в порядке старшинства (Nicho, 2018):

а. Председатель совета директоров.

б. Член совета директоров.

в. Главный исполнительный директор.

г. Президент.
д. Исполнительный вице-президент.
е. Старший вице-президент.
ж. Вице-президент.
з. Исполнительный директор.
и. Старший директор.
к. Директор.
л. Старший менеджер.
м. Менеджер.
н. Супервайзер.

В приведенном списке показаны некоторые ранги иерархии, но в крупных организациях существуют и другие должности, такие как первый вице-президент, генеральный директор или помощник директора. Кроме того, обязанности во многом похожи на роли, определяющие задачи, выполнения которых ожидают от сотрудника. В целях информационной безопасности организации распределяют конкретные роли и обязанности между сотрудниками, что гарантирует выполнение стратегии и целей организации в области ИБ.

2.1. Стандартный метод управления организациями

Многие организации используют собственные методы управления информационной безопасностью, например, проводят различные меры в этой области. Однако существует стандартный метод, который широко используется для определения ролей и обязанностей в организациях, – матрица распределения ответственности RACI (Responsible – Accountable – Consulted – Informed). Она служит для распределения ролей между сотрудниками и командами для выполнения задач и действий. Кроме того, матрица в общих чертах описывает, кто и что должен делать в данной организации. Например, менеджер проекта должен также выполнять обязанности аналитика по безопасности. Кроме того, согласно матрице RACI обязанности каждого сотрудника на любом уровне старшинства распределяются следующим образом (Bettwy et al., 2016):

i. Исполнитель: сотрудник, который отвечает за непосредственное выполнение задания.

ii. Ответственный: сотрудник, который руководит работой исполнителя и отвечает за результат выполнения задания.

iii. Консультант: специалист либо эксперт в предметной области, с которым можно проконсультироваться по какому-либо вопросу.

iv. Наблюдатель, информируемое лицо: сотрудник, которого надлежит уведомлять во время или до начала действия.

В табл. 1 приведен пример распределения ролей и обязанностей в организации. Прежде всего, каждый сотрудник в организации должен иметь должность и принадлежать к тому или иному подразделению. Кроме того, все сотрудники должны пройти специальный курс обучения, который даст им набор навыков для выполнения поставленных задач. Согласно матрице RACI, каждый сотрудник имеет свои собственные задачи, что и называется разделением обязанностей (Separation of Duties, SoD). SoD означает, что ни один сотрудник не имеет полного контроля над критическим процессом деятельности, который может повлиять на функциональность организации. Например, при предоставлении сотруднику учетной записи лицо, предоставляющее,

утверждающее и запрашивающее данные, не должно принадлежать к тому же отделу в целях предотвращения конфликта интересов (Von Solms et al., 2011).

Таблица 1. Распределение ролей и обязанностей в матрице RACI

Деятельность	Исполнитель	Ответственный	Консультант	Наблюдатель
Контроль аккаунта пользователя	IA	IAM	AO	IT SD, IT SM, EUM
Предоставление аккаунта пользователя	IT SD	IT SM	AO	IT SD, EUM, ST
Утверждение аккаунта пользователя	AO	COO	EUM, ST	EU, IA, IT SD
Запрос на аккаунт пользователя	EU	EUM	IT SD, EUM	AO, ST

* EU – конечный пользователь, EUM – менеджер конечного пользователя, SD – отдел обслуживания, AO – владелец активов, ST – отдел безопасности, IA – внутренний аудит, SM – менеджер по обслуживанию, IAM – менеджер внутреннего аудита.

Источник: (Von Solms et al., 2011).

2.2. Стандарты и принципы безопасности в организациях

Успешная организация действует в рамках правильно разработанной системы УИБ, основанной на стандартах, которые соответствуют ее видению и стратегии. Однако не так-то просто разработать стратегию, которая включала бы в себя политику компании, стандарты, процессы и матрицы в соответствии с общим видением организации. В данном разделе представлены стандарты, которые применяются в таких организациях мирового масштаба, как Google, Meta[4], Amazon и т. д. Более того, если специалист по безопасности вместе с руководителями высшего звена решают разработать структуру УИБ для своей организации и ограничиваются только системой контроля, это считается ошибкой. Мы предлагаем использовать данную структуру УИБ в качестве примера и изучить мировые стандарты и средства контроля безопасности, чтобы избежать ошибок и обеспечить хороший старт в управлении организацией. В табл. 2 перечислены стандарты и системы контроля, которые могут быть полезны в качестве отправной точки для разработки системы УИБ для государственных и частных организаций (Tan et al., 2010; Fazlida & Said, 2015; Ula et al., 2017).

Таблица 2. Некоторые стандарты и принципы контроля

№	Стандарты и принципы	Пояснение
1	Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST)	Используется Министерством торговли США для стандартизации в области экономической безопасности, инноваций, промышленности и технологий
2	Международная организация по стандартизации/Международная электротехническая комиссия (International Organization for Standardization/ International Electrotechnical Commission, ISO/IEC)	Два основных международных стандарта в области информационной безопасности, технологий, промышленности и деловой практики

[4] Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

Окончание табл. 2

№	Стандарты и принципы	Пояснение
3	Контрольные точки в области информационных и смежных технологий (Control Objectives for Information and Related Technologies, COBIT)	Система управления сектором ИТ и предприятиями, которая устанавливает ряд руководящих принципов и лучшие практики для ИТ-организаций
4	Стандарт безопасности данных в области платежных карт (Payment Card Industry Data Security Standard, PCI-DSS)	Стандарты информационной безопасности, разработанные для защиты конфиденциальной информации платежных карт
5	Закон о переносимости и подотчетности в сфере медицинского страхования (Health Insurance Portability and Accountability Act, HIPAA)	Закон США, защищающий конфиденциальность информации о здоровье людей и обеспечивающий безопасность медицинских данных
6	Форум по информационной безопасности (Information Security Forum, ISF)	Набор средств контроля безопасности и лучших практик, используемых для управления рисками в сфере информационной безопасности
7	Библиотека инфраструктуры информационных технологий (Information Technology Infrastructure Library, ITIL)	Система ИТ-услуг, разработанная для целей управления, включая управление ИТ-инфраструктурой, средой, услугами и процессами

Источник: (Ula et al., 2017).

3. Лучшие системы управления информационной безопасностью

В данном разделе представлен ряд ведущих систем в области УИБ и кибербезопасности. Такие системы есть и в арабских странах. Например, Объединенные Арабские Эмираты и Саудовская Аравия являются примером для подражания в этой важной области. Ниже перечислены системы УИБ, законы и правила контроля информации ряда стран (Shingarev & Kazakova, 2021; Creemers, 2023; Priyadarshini & Cotton, 2022; Carr & Tanczer, 2018; Singh & Alshammari, 2020; Al Neaimi et al., 2015):

а) Россия: в систему входит Федеральная служба по техническому и экспортному контролю (ФСТЭК), обеспечивающая безопасность продукции; действует Федеральный закон № 149-ФЗ для защиты данных; важную роль в обеспечении кибербезопасности играет Федеральная служба безопасности (ФСБ). Согласно законодательству, информация российских граждан должна храниться внутри страны (Shingarev & Kazakova, 2021);

б) Китай: в систему УИБ входит Министерство общественной безопасности (МОБ), которое следит за информационной безопасностью в Китае. Кроме того, в 2017 г. в Китае приняты Закон о кибербезопасности и Закон о национальной безопасности (NSL), а также Закон об управлении киберпространством Китая (CAC), который регулирует работу Интернета (Creemers, 2023);

в) США: система УИБ включает Федеральный закон об управлении информационной безопасностью (FISMA) и Закон о повышении кибербезопасности (CEA) от 2014 г. Кроме того, действует Национальный институт стандартов и технологий (NIST), который устанавливает стандарты. Агентство по кибербезопасности и инфраструктурной безопасности (CISA) координирует деятельность таких структур, занимающихся вопросами кибербезопасности, как Агентство национальной безопасности (АНБ) (Priyadarshini & Cotton, 2022);

г) Великобритания: система УИБ включает акты и стратегии Национальной стратегии кибербезопасности (NCSC) и Закон о защите данных (DPA) 2018 г. Кроме того, Закон о неправомерном использовании компьютеров (CMA) 1990 г. предусматривает киберпреступления. Правительство Великобритании участвует в международном сотрудничестве в области кибербезопасности (Carr & Tanczer, 2018);

д) Саудовская Аравия: система УИБ включает Закон о кибербезопасности Саудовской Аравии (SACL) от 2019 г., который контролируется Комиссией по коммуникациям, космосу и технологиям (CITC) и Национальным управлением по кибербезопасности (NCA). Центральный банк Саудовской Аравии (SAMA) осуществляет надзор за операциями в финансовом секторе (Singh & Alshammari, 2020);

е) ОАЭ: система УИБ включает Закон о кибербезопасности ОАЭ от 2019 г. и надзор со стороны Национального управления электронной безопасности (NESA) и Управления по регулированию телекоммуникаций и цифрового управления (TRDA). Вопросами надзора за кибербезопасностью в Дубае занимается Дубайский англоязычный колледж (DESC) (Al Neaimi et al., 2015).

4. Предлагаемая система управления информационной безопасностью

Прежде чем предлагать какую-либо новую систему или развивать существующую, необходимо объяснить сущность двух фундаментальных понятий: управления и корпоративного управления. Управление связано с защитой интересов собственников путем руководства, управления и надзора от их имени, при этом совет директоров выступает в качестве их представителей. Корпоративное управление определяется как реакция на различия интересов руководства и собственников в частных и государственных организациях. Кроме того, оно направлено на поддержание этого различия через стимулирование руководства и совета директоров преследовать цели, которые соответствуют интересам компании и ее акционеров.

Предлагаемая структура УИБ должна включать ряд элементов, обеспечивающих эффективную защиту и управление информационными активами организации, обеспечение дисциплины собственников и руководства, а также предоставление собственникам полномочий по контролю за деятельностью организации. Кроме того, создавая безопасную среду для обмена и хранения информации, организации могут не только повысить производительность, потребительские преимущества и эффективность бизнеса, но и обеспечить меры безопасности. И наоборот, любая небезопасная рабочая среда представляет собой значительный риск, который может нанести существенный ущерб корпорациям и правительствам, а также негативно отразиться на гражданах и потребителях. Это особенно важно для предприятий, работающих в таких критически важных сферах, как финансы, электроэнергетика, банковское дело или здравоохранение, где ставки исключительно высоки. В табл. 3 показаны основные вопросы организации эффективной системы УИБ.

Таблица 3. Основные вопросы/действия по организации эффективной системы УИБ

Действующие лица/ Действия	Руководитель предприятия	Руководитель подразделения	Старший управляющий	ИТ-директор/директор по информационной безопасности
Управление/движущие силы бизнеса	Что от меня требуется? Что я должен обязательно сделать?			
Роли и ответственность	Как я могу выполнить свои задачи?			
Измерения/Аудит	Насколько эффективно я могу выполнить свои задачи? Что я должен изменить?			

Система УИБ служит инструментом реализации стратегии и видения руководителей высшего звена для достижения высокой эффективности бизнес-операций и принятия решений в организациях. В их компетенцию входят управление всей деятельностью организации и защита ее данных и активов путем обеспечения эффективной интеграции информационной безопасности в масштабах всей организации.

Чтобы разработать эффективную систему УИБ, которая может быть утверждена и принята во всем мире, необходимо принять во внимание ряд глобальных законов и норм. Они могут дать большое преимущество благодаря своей структуре и продуманности, если опираться на них как на законодательный опыт других стран. В табл. 4 приведены некоторые ключевые законы и нормы, которые использовались в разных странах мира для регулирования информационной безопасности.

Таблица 4. Примеры законов и нормативных актов, принятых в разных странах мира[5]

№	Законы и нормы	Пояснения
1	Общий регламент по защите данных (General Data Protection Regulation, GDPR)	Обязывает организации защищать личные данные граждан на территории Европейского союза и устанавливает строгие требования к конфиденциальности и безопасности данных
2	Закон Калифорнии о защите персональных данных потребителей (California Consumer Privacy Act, CCPA)	Распространяется на компании, которые собирают личную информацию жителей Калифорнии, и требует принятия мер по защите конфиденциальности и безопасности такой информации
3	Закон Сарбейнса – Оксли (Sarbanes – Oxley Act, SOX)	Требует создания и поддержания внутреннего контроля над финансовой отчетностью компаний, включая меры по защите целостности и конфиденциальности финансовых данных
4	Федеральный закон об управлении информационной безопасностью (Federal Information Security Management Act, FISMA)	Федеральный закон США, который устанавливает требования безопасности для федеральных информационных систем и обеспечивает основу для управления рисками кибербезопасности в федеральных агентствах
5	Сертификация модели кибербезопасности (Cybersecurity Maturity Model Certification, CMMC)	Разработана Министерством обороны США для оценки и повышения уровня кибербезопасности подрядчиков и субподрядчиков оборонной отрасли
6	Законы о защите данных (Data Protection Laws, DPL)	В разных странах приняты свои законы о защите данных, например, Закон о защите персональной информации и электронных документов (PIPEDA) в Канаде и Закон о защите персональных данных (PDPA) в Сингапуре

Заключение

В данной работе предлагается новая система УИБ (включая кибербезопасность) для защиты информации и активов государственных и частных организаций, использующая преимущества ряда законов и нормативных актов. Эту систему можно сравнить с существующими системами, которые были внедрены в организациях по всему миру. Она нацелена на достижение баланса между постоянным совершенствованием и управлением рисками и соответствует бизнес-модели организации, основанной на требованиях нормативных актов и законов. Подчеркивается,

[5] Manning, W. (2010). CISM Certified Information Security Manager certification exam preparation course in a book for passing the CISM: The how to pass on your first try certification study guide. Brisbane, Australia: Emereo Pty Ltd.

что любая организация должна иметь свою собственную систему УИБ, внедрение которой является задачей специального комитета (совета директоров). Для последовательного внедрения УИБ в стране комитеты во всех организациях должны быть связаны друг с другом вышестоящим комитетом по УИБ или кибербезопасностью, который должен осуществлять общее управление. Кроме того, данная структура УИБ выступает в качестве инструмента для реализации управления информационной безопасностью, а также обеспечивает эффективность всего процесса в соответствии с целями и задачами бизнеса. Таким образом, предложенная структура УИБ составляет реальную программу безопасности, которая может быть применена к любой частной и государственной организации.

Список литературы

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity (*pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Сведения об авторах

Хади Мусадак Ахмед – магистр наук (инженер систем управления), кафедра управления и системной инженерии, Технологический университет
Адрес: Аль-Вейда, г. Багдад, Ирак
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Абдулредха Мохаммед Наджм – магистр компьютерных наук, кафедра компьютерных наук, Багдадский университет
Адрес: Аль-Джадрийя, г. Багдад, Ирак
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 16 апреля 2024 г.
Дата одобрения после рецензирования – 4 мая 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:34.05:004.056.5
EDN: https://elibrary.ru/xujvtm
DOI: https://doi.org/10.21202/jdtl.2025.6

Universal Information Security Governance System: Organizational and Legal Principles

Musadaq Ahmed Hadi ✉
University of Technology, Baghdad, Iraq

Mohammed Najm Abdulredha
University of Baghdad, Baghdad, Iraq

Keywords

cybersecurity,
digital technologies,
information protection,
information security governance,
information security,
information technologies,
law,
legal regulation,
legislation,
organizational structure

Abstract

Objective: to develop universal organizational and legal principles for building an information security governance system that will allow each organization to create its own effective information security governance system, taking into account its unique business goals and tasks.

Methods: the research integrates the key elements of information security governance, such as vision, strategy, goals, policies, standards, processes, and matrices. Vision and goals set the direction of an organization's development; policies and standards provide a conceptual framework for information protection; processes allow for systematic achievement of objectives; and matrices provide tools for evaluating and monitoring the entire structure. The proposed principles are consistent with international standards, regulatory requirements, and best practices in the field of information security.

Results: the research showed that the developed information security governance system allows for a clear distribution of roles and responsibilities among the employees, ensuring effective implementation of the governance system. The authors also analyzed the existing principles of information security, integrating them into a security strategy that meets the corporate goals. The proposed universal system complies with regulatory legal requirements and can be adapted for organizations of any scale and profile.

✉ Corresponding author

Scientific novelty: the paper represents a practical approach to the implementation of an information security governance system based on the authors' experience, international standards, control systems and legal acts. Unlike existing approaches, the proposed system is flexible and can be adapted to any organization, which makes it a universal tool for information security governance.

Practical significance: the research provides a structured approach to creating a universal information security governance system that can be used by organizations lacking knowledge and resources to implement such initiatives. The authors propose a general structure that can be adapted depending on the organization's assets, the employees' training and awareness of information security issues. This makes the paper a valuable resource for professionals seeking to increase information security in their organizations.

For citation

Hadi, M. A., & Abdulredha, M. N. (2025). Universal Information Security Governance System: Organizational and Legal Principles. *Journal of Digital Technologies and Law, 3*(1), 125–142. https://doi.org/10.21202/jdtl.2025.6

References

Al Neaimi, A., Ranginya, T., & Lutaaya, P. (2015). A framework for effectiveness of cyber security defenses, a case of the United Arab Emirates (UAE). *International Journal of Cyber-Security and Digital Forensics*, *4*(1), 290–301. https://doi.org/10.17781/p001502

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges AND CRITICAL SUCCESS FACTORS: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

Bettwy, G., Beevers, M., & Williams, M. (2016). *CISM Review Manual Certified Information Security manager*. Rolling Meadows, Ill: ISACA.

Carcary, M., Renaud, K., McLaughlin, S., & O'Brien, C. (2016). A framework for Information Security Governance and Management. *IT Professional*, *18*(2), 22–30. https://doi.org/10.1109/mitp.2016.27

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: An analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Corriss, L. (2010). Information security governance. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 35–41). https://doi.org/10.1145/1920320.1920326

Creemers, R. (2023). Cybersecurity law and regulation in China: Securing the smart state. *China Law and Society Review*, *6*(2), 111–145. https://doi.org/10.1163/25427466-06020001

Fazlida, M. R., & Said, J. (2015). Information security: Risk, governance and implementation setback. *Procedia Economics and Finance*, *28*, 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Hadi, M. A., Abdulredha, M. N., & Hasan, E. (2023). Introduction to ChatGPT: A new revolution of artificial intelligence with machine learning algorithms and cybersecurity. *Science Archives*, *04*(04), 276–285. https://doi.org/10.47587/sa.2023.4406

Johnston, A. C., & Hale, R. (2009). Improved security through information security governance. *Communications of the ACM*, *52*(1), 126–129. https://doi.org/10.1145/1435417.1435446

Moulton, R., & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580–584. https://doi.org/10.1016/s0167-4048(03)00705-3

Nicho, M. (2018). A process model for implementing Information Systems Security governance. *Information & Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ics-07-2016-0061

Ohki, E., Harada, Y., Kawaguchi, Sh., Shiozaki, T., & Kagaya, T. (2009). Information security governance framework. *Proceedings of the first ACM workshop on Information security governance* (pp. 1–6). https://doi.org/10.1145/1655168.1655170

Priyadarshini, I., & Cotton, C. (2022). Cyber laws in the United States. *Cybersecurity (*pp. 157–237). https://doi.org/10.1201/9781003187127-6

Rao, U. H., & Nayak, U. (2014). History of computer security. *The InfoSec Handbook* (pp. 13–25). https://doi.org/10.1007/978-1-4302-6383-8_2

Rastogi, R., & von Solms, R. (2005). Information security governance – a re-definition. *Security Management, Integrity, and Internal Control in Information Systems* (pp. 223–236). https://doi.org/10.1007/0-387-31167-x_14

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology*, *58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, *43*, 90–110. https://doi.org/10.1016/j.cose.2014.03.004

Shingarev, A., & Kazakova, A. (2021). The Russian Federation's approach to Cybersecurity. *The Oxford Handbook of Cyber Security* (pp. 672–684). https://doi.org/10.1093/oxfordhb/9780198800682.013.44

Singh, H. P., & Alshammari, T. S. (2020). An institutional theory perspective on developing a cyber security legal framework: A case of Saudi Arabia. *Beijing Law Review*, *11*(03), 637–650. https://doi.org/10.4236/blr.2020.113039

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010). Information security governance: When compliance becomes more important than security. *Security and Privacy – Silver Linings in the Cloud* (pp. 55–67). https://doi.org/10.1007/978-3-642-15257-3_6

Ula, M., Ula, M., & Fuadi, W. (2017). A method for Evaluating Information Security Governance (ISG) components in banking environment. *Journal of Physics: Conference Series*, *812*, 012031. https://doi.org/10.1088/1742-6596/812/1/012031

Von Solms, S. H., & von Solms, R. (2010). *Information security governance*. New York, United States: Springer.

Von Solms, R., Thomson, K.-L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *Information Security for South Africa* (pp. 1–6). https://doi.org/10.1109/issa.2011.6027522

Wu, M., Aranovich, R., & Filkov, V. (2021). Evolution and differentiation of the cybersecurity communities in three social question and answer sites: A mixed-methods analysis. PLOS ONE, 16(12). https://doi.org/10.1371/journal.pone.0261954

Authors information

Musadaq Ahmed Hadi – MSc. (Control Engineer), Control and Systems Engineering Department, University of Technology
Address: Al-Wehda, Baghdad, Iraq
E-mail: musadaq.ahmed@alshaab.edu.iq
ORCID ID: https://orcid.org/0000-0002-3884-495X
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57117413800
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JZT-4113-2024
Google Scholar ID: https://scholar.google.com/citations?user=wcrA7n8AAAAJ

Mohammed Najm Abdulredha – MSc. (Computer Science), Department of Computer Science, University of Baghdad
Address: Al-Jadriya, Baghdad, Iraq
E-mail: mohammed.najm.422@gmail.com
ORCID ID: https://orcid.org/0009-0007-8441-3505
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57226709471
WoS Researcher ID: https://www.webofscience.com/wos/author/record/KIJ-3538-2024
Google Scholar ID: https://scholar.google.ru/citations?user=-oXQXKEAAAAJ

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interest

The authors declare no conflict of interest.

Thematic rubrics

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

Article history

Date of receipt – April 16, 2025
Date of approval – May 4, 2025
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025

Научная статья
УДК 34:004:17:004.8:342.7
EDN: https://elibrary.ru/egkppn
DOI: https://doi.org/10.21202/jdtl.2025.7

Искусственный интеллект в здравоохранении: баланс инноваций, этики и защиты прав человека

Педро Мигель Алвес Рибейро Коррейя ✉
Коимбрский университет, Коимбра, Португалия

Рикардо Лопес Динис Педро
Лиссабонский университет, Лиссабон, Португалия

Сусана Видейра
Лиссабонский университет, Лиссабон, Португалия

Ключевые слова

защита данных,
здравоохранение,
искусственный интеллект,
права человека,
право,
правовое регулирование,
предиктивная аналитика,
фундаментальные права,
этика,
этическое регулирование

Аннотация

Цель: определить ключевые этические, правовые и социальные вызовы, связанные с использованием искусственного интеллекта в здравоохранении, а также разработать рекомендации для создания адаптивных правовых механизмов, способных обеспечить баланс между инновациями, этическим регулированием и защитой фундаментальных прав человека.

Методы: в ходе исследования был реализован многоаспектный методологический подход, интегрирующий классические правовые методы анализа с современными инструментами сравнительного правоведения. Данное исследование охватывает как фундаментальные основы правового регулирования цифровых технологий в медицинской сфере, так и глубокий анализ этических, правовых и социальных импликаций внедрения искусственного интеллекта в систему здравоохранения. Такой комплексный подход позволил обеспечить всестороннее понимание проблематики и сформировать обоснованные выводы относительно перспектив развития данной области.

Результаты: выявлен ряд серьезных проблем, связанных с использованием искусственного интеллекта в здравоохранении. К ним относятся необъективность данных, непрозрачность сложных алгоритмов и риски нарушения неприкосновенности частной жизни. Эти проблемы могут подорвать доверие общества к технологиям искусственного интеллекта и усугубить неравенство в доступе к медицинским услугам. Авторы приходят к выводу, что интеграция искусственного интеллекта в систему здравоохранения должна осуществляться с учетом фундаментальных прав, таких как защита данных и запрет дискриминации, а также соответствовать этическим нормам.

✉ Контактное лицо

Научная новизна: состоит в предложении эффективных механизмов управления для снижения рисков и максимизации потенциала искусственного интеллекта в кризисных ситуациях. Особое внимание уделяется регулятивным мерам, таким как оценка влияния, предусмотренная Законом об искусственном интеллекте. Эти меры играют ключевую роль в выявлении и минимизации рисков, связанных с высокорисковыми системами искусственного интеллекта, обеспечивая соблюдение этических норм и защиту основных прав.

Практическая значимость: заключается в разработке адаптивных правовых механизмов, которые поддерживают демократические нормы и оперативно реагируют на возникающие вызовы в области общественного здравоохранения. Предложенные механизмы позволяют достичь баланса между использованием искусственного интеллекта для управления кризисными ситуациями и сохранением прав человека. Это способствует укреплению доверия к системам искусственного интеллекта и их устойчивому положительному влиянию на общественное здравоохранение.

Для цитирования

Коррейя, П. М. А. Р., Педро, Р. Л. Д., & Видейра, С. (2025). Искусственный интеллект в здравоохранении: баланс инноваций, этики и защиты прав человека. *Journal of Digital Technologies and Law*, *3*(1), 143–180. https://doi.org/10.21202/jdtl.2025.7

Содержание

Введение

В настоящее время борьба с болезнями и пандемиями ведется на уровне врачей-практиков, учреждений здравоохранения и целых государств. Может ли искусственный интеллект (далее – ИИ) помочь нам в этой сфере? Какие ограничения накладывает при этом необходимость соблюдения фундаментальных прав?

На протяжении всей истории человечество сталкивалось с разрушительными последствиями эпидемий и пандемий, от бубонной чумы до испанского гриппа. Вспышки болезней изменяли целые сообщества и даже ставили под сомнение само существование человека. Сегодня, когда мы живем во все более взаимосвязанном мире, все более реальной становится угроза новых и быстро распространяющихся болезней. Глобализация все чаще выступает в роли обоюдоострого меча, способствуя как сотрудничеству, так и быстрой передаче патогенов через границы государств (Jones et al., 2008; Morse et al., 2012).

Искусственный интеллект сегодня рассматривается как новое оружие в этой извечной борьбе. Эта мощная революционная технология (или совокупность технологий), некогда относившаяся к области научной фантастики, обладает огромным потенциалом для кардинального изменения методов борьбы с эпидемиями и пандемиями. Она может стать мощным оружием в нашем арсенале для борьбы с болезнями. С помощью методов искусственного интеллекта можно будет анализировать огромные массивы данных, предсказывать вспышки и исход болезней, ускорять поиск лекарств и даже персонализировать стратегии лечения (Syrowatka et al., 2021). По крайней мере, так принято считать.

К примеру, искусственный интеллект можно использовать для прогнозирования чрезвычайных ситуаций, поскольку он способен просеивать огромный объем информации из социальных сетей, новостных сообщений и даже спутниковых снимков, выявляя ранние признаки вспышки заболевания до того, как она перерастет в полномасштабную пандемию. Нетрудно представить, как система искусственного интеллекта обнаруживает резкий рост числа запросов о симптомах, похожих на грипп, в определенном регионе и немедленно начинает исследовать это явление, что потенциально может в зародыше пресечь вспышку заболевания (Wong et al., 2023).

Другой пример – использование искусственного интеллекта для ускорения поиска лекарств (если фармацевтические компании вообще собираются делать это, а не только облегчать хронические заболевания, что приносит им постоянный доход). Открытие химических соединений (в том числе вакцин) для медицинских целей всегда было медленным и сложным процессом; часто проходят годы, пока не будет получен результат, а иногда он и вовсе не достигается. Искусственный интеллект может революционизировать этот процесс путем анализа молекулярных структур веществ для выявления потенциальных кандидатов в лекарственные препараты или для перепрофилирования существующих лекарств в новые. Это значительно сократит время, необходимое для того, чтобы жизненно важные лекарства попали к пациентам (Matsuzaka & Yashiro, 2022).

Еще одна возможность состоит в применении индивидуального подхода к лечению. Искусственный интеллект может анализировать индивидуальные генетические особенности и историю болезни пациента, предсказать его реакцию на различные варианты лечения. Это откроет пути к персонализированной медицине и позволит врачам адаптировать планы лечения для достижения максимальной эффективности (Topol, 2019).

Также искусственный интеллект может использоваться в данном контексте для предсказания траектории развития вспышки заболевания или пандемии. Модели ИИ способны анализировать данные о развитии и характеристиках заболевания, что позволяет чиновникам системы здравоохранения стратегически распределять ресурсы и осуществлять целенаправленные меры для сдерживания распространения болезни (Ferguson et al., 2006).

Последний пример (из множества других, не перечисленных здесь) – использование искусственного интеллекта для улучшения отслеживания контактов, поскольку ИИ может анализировать данные о контактах и поездках, точно определяя лиц с высоким риском заражения. Это поможет медицинским работникам определить приоритетность тестирования и карантинных мер, потенциально сдерживая распространение патогена (Fetzer & Graeber, 2021).

Однако этот путь не лишен преград. Предвзятость данных, «черного ящика», или «серого ящика», сложные алгоритмы, а также постоянно присутствующий риск чрезмерной зависимости от искусственного интеллекта – все это создает потенциальные и значительные трудности (DeCamp & Tilburt, 2019).

Хотя мы перечислили ряд потенциальных возможностей искусственного интеллекта, данная работа посвящена не столько его преимуществам в борьбе с болезнями, эпидемиями или пандемиями, сколько критическим соображениям и предостережениям, которые следует учитывать пользователям по мере того, как использование этих подходов все чаще становится предметом размышлений. Мы рассмотрим различные проблемы, с которыми столкнемся, прежде чем искусственный интеллект сможет стать маяком надежды в мире, над которым постоянно нависает угроза широкомасштабных, всеобщих и острых вспышек заболеваний.

Кроме того, мы проанализируем влияние ИИ на фундаментальные права, а также проблему использования искусственного интеллекта для борьбы с пандемией и ее связь с соблюдением фундаментальных прав.

1. Использование искусственного интеллекта в борьбе с пандемиями и причины неудач в этой области

Потенциальные возможности ИИ неразрывно связаны с проблемами, которые необходимо решать. Широко известно высказывание Джорджа Бокса о том, что «все модели ошибочны, но некоторые из них полезны» (Box, 1979). Неудивительно, что, несмотря на сильные стороны моделей искусственного интеллекта, их эффективность сдерживается рядом ограничений, которые могут превратить эти решения в обоюдоострый меч.

Один из главных недостатков моделей искусственного интеллекта заключается в том, что эти модели хороши лишь настолько, насколько хороши данные, на которых они обучаются. Неточные, неполные или предвзятые данные могут привести к ненадежным и потенциально вредным результатам (Gianfrancesco et al., 2018). Ограниченный доступ к медицинским данным в режиме реального времени в некоторых регионах или проблемы с конфиденциальностью еще больше снижают возможности искусственного интеллекта.

Еще одна проблема широко известна как свойство «черного ящика» или, в более мягкой формулировке, свойство «серого ящика». Внутренняя работа сложных алгоритмов чрезвычайно сложна, и люди не всегда способны понять процессы принятия

решений искусственным интеллектом. Эта непрозрачность, в свою очередь, подрывает доверие и усложняет задачу обнаружения и устранения скрытых предубеждений и различных других проблем (Mittelstadt et al., 2016).

Ошибкой было бы также чрезмерно полагаться на значительные возможности моделей искусственного интеллекта, не признавая их фундаментальных ограничений. Другими словами, необходимо уделять должное внимание основополагающим стратегиям общественного здравоохранения, таким как отслеживание контактов, вакцинация и кампании по повышению осведомленности населения. Все эти подходы проверены временем и должны продолжать играть жизненно важную роль в эффективном управлении вспышками заболеваний (Silva et al., 2022).

2. Примеры неудач искусственного интеллекта: извлеченные уроки и дальнейшие действия

Пандемия COVID-19 стала полигоном для испытания искусственного интеллекта в борьбе с болезнями, но результаты оказались неоднозначными. Рассмотрим ряд примеров.

В самом начале пандемии некоторые модели искусственного интеллекта сильно переоценили распространение вируса из-за ограниченности исходных данных и быстро меняющейся ситуации. Это привело к панике и выделению ненужных ресурсов. В других случаях чат-боты на базе искусственного интеллекта, созданные для ответов на вопросы в области здравоохранения, были перегружены и иногда предоставляли неверную информацию. Это подчеркивает необходимость наличия надежных обучающих данных и четких ограничений для приложений с искусственным интеллектом (Bajwa et al., 2021; Gürsoy & Kaya, 2023).

Таким образом, можно утверждать, что, только признав ограничения искусственного интеллекта и сосредоточившись на принципах ответственного развития, человечество сможет использовать его возможности для более здорового будущего. Для создания надежных моделей искусственного интеллекта крайне важны приоритетность качества данных и ответственная практика их сбора, а также устранение предвзятости данных и обеспечение их конфиденциальности. Разработка надежных методов снижения предвзятости алгоритмов искусственного интеллекта, основанных на проверке справедливости и расширении спектра данных, также должна помочь в выявлении и устранении потенциальной предвзятости на самых начальных этапах. Необходимо поддерживать исследования в области объяснимого искусственного интеллекта (explainable artificial intelligence, XAI). Это поможет заинтересованным сторонам понять, как модели искусственного интеллекта приходят к своим выводам, укрепит доверие и позволит выявлять потенциальные проблемы на ранней стадии (Jobin et al., 2019).

Важно придерживаться сбалансированных подходов, когда искусственный интеллект используется наряду с традиционными мерами в области общественного здравоохранения и дополняет, а не заменяет их. Решая эти проблемы и поощряя ответственное развитие искусственного интеллекта, заинтересованные стороны смогут пользоваться всеми его возможностями и стать лучше подготовленными к будущим пандемиям (Benke & Benke, 2018). Искусственный интеллект может стать мощным оружием в арсенале человечества, но только при условии его разумного использования, как показано ниже.

3. Проблема «мусор на входе – мусор на выходе»

Фундаментальный принцип искусственного интеллекта, в частности машинного обучения, можно сформулировать так: «мусор на входе – мусор на выходе» (Breiman, 2001).

Рассмотрим основные типы «мусорных» данных. Во-первых, данные могут быть неточными. К ним относятся орфографические ошибки, опечатки, фактические ошибки, устаревшая информация (Halevy et al., 2009). Представим себе искусственный интеллект, обученный на новостных статьях с большим количеством опечаток; ему будет трудно понимать язык. Во-вторых, данные могут быть неполными. Отсутствующие значения или отдельные данные будут искажать понимание модели (Little & Rubin, 2019). Например, модель для прогнозирования оттока клиентов (причин, почему пациенты решают не возвращаться в данную больницу) пропустит важные данные, если не будет учитывать отзывы клиентов. В-третьих, данные могут быть необъективными. Данные, необъективно представляющие определенную группу, приведут к дискриминационным результатам (Berk, 1983). Так, если искусственный интеллект, используемый для принятия решений о приеме на работу, обучали в основном на резюме мужчин, то он будет отдавать предпочтение кандидатам-мужчинам. И в-четвертых, данные могут быть нерелевантными. Информация, не имеющая отношения к решаемой задаче, исказит работу модели (Greiner et al., 1997). Так, искусственный интеллект для анализа настроения (понимания эмоций в тексте) в психиатрической клинике может быть перегружен нерелевантными эмодзи в представленном наборе данных.

Это также помогает понять, каковы могут быть последствия «мусора на входе». Во-первых, поддерживается предвзятость: искусственный интеллект может усиливать существующие в обществе предубеждения, если таковые содержатся в обучающих данных (Bazarkina & Pashentsev, 2020). Это может негативно отразиться на результатах деятельности ИИ в таких областях, как одобрение кредитов, распознавание лиц и прогнозирование в сфере уголовного правосудия. Далее, снижается точность и надежность, поскольку модели, обученные на неточных данных, будут выдавать ненадежные результаты (Shin & Park, 2019). Представьте себе искусственный интеллект для прогнозирования патологий, обученный на неверных показаниях температуры у пациентов; его диагноз будет неточным. Кроме того, при обучении моделей на неверных данных значительные ресурсы будут потрачены впустую (Hulten, 2018).

Необходимо знать основные методы борьбы с «мусором на входе». С одной стороны, нужно вкладывать средства в очистку и обработку данных. Для обеспечения качества данных используются такие методы, как проверка данных, исправление ошибок и фильтрация. Это трудоемкий процесс, но крайне важный для получения надежного искусственного интеллекта (Wang & Shi, 2011). С другой стороны, для решения такой проблемы, как неполнота данных, необходимо использовать синтетические данные в дополнение к существующим базам данных (Mumuni & Mumuni, 2022). Например, создание реалистичных изображений различных лиц помогает уменьшить предвзятость при распознавании лиц. Другой пример – использование алгоритмических методов обнаружения предвзятости для выявления и снижения предвзятости в самих алгоритмах искусственного интеллекта. Сюда входит анализ процесса принятия решений моделью с целью выявления скрытых предубеждений

(Kordzadeh & Ghasemaghaei, 2022). Еще одна техника, направленная на повышение прозрачности моделей искусственного интеллекта, – это объясняемый искусственный интеллект. Она позволяет понять, как модель приходит к своим выводам, и выявить потенциальные предубеждения или ошибки (Arrieta et al., 2020).

Решение проблемы «мусор на входе – мусор на выходе» критически важно для создания надежного и этичного искусственного интеллекта в будущем. По мере того как искусственный интеллект все больше интегрируется в жизнь каждого человека, обеспечение качества данных и уменьшение их предвзятости приобретает огромное значение (Jobin et al., 2019). В этом направлении уже прилагаются определенные усилия. Стандартизация и регулирование не решат проблему полностью, но могут помочь в ее решении. Разработка руководящих принципов и правил ответственной разработки и внедрения искусственного интеллекта повышает качество и надежность данных[1]. Также ведется просветительская и информационная работа с населением. Повышение осведомленности о потенциальных недостатках искусственного интеллекта и важности ответственного подхода к разработке способствует укреплению общественного доверия (Kandlhofer et al., 2023). Кроме того, междисциплинарное сотрудничество между разработчиками искусственного интеллекта и экспертами, включая специалистов в области этики, науки о данных, государственных деятелей, имеет решающее значение для создания надежных и ответственных систем искусственного интеллекта (Bisconti et al., 2023). Это еще одна тенденция, которая может предотвратить или замедлить попадание в ловушку «мусор на входе – мусор на выходе».

4. Проблема устойчивости, о которой почти не говорят

Ключевым фактором должна стать устойчивость решений в области искусственного интеллекта.

Первостепенное значение имеет энергопотребление. Обучение большой языковой модели, такой как GPT-3, требует столько же энергии, сколько несколько автомобилей за весь срок службы. По оценкам некоторых исследований, энергопотребление при обучении одной большой языковой модели составляет около 1,5 МВт·ч[2]. Центры обработки данных, в которых размещаются системы искусственного интеллекта, по самым скромным оценкам, потребляют от 1 до 3 % мирового объема электроэнергии[3].

Кроме того, все большую озабоченность вызывает потребление воды. Центры обработки данных в значительной степени зависят от воды для охлаждения: по оценкам, только в Соединенных Штатах Америки они потребляют до 1,7 млрд галлонов воды в год[4]. Расход воды при работе искусственного интеллекта может быть значительным даже для отдельных пользователей. Один запрос к большой языковой модели расходует небольшую бутылку воды[5].

---

1 European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Legislative Instruments (COM(2021) 206 final). https://clck.ru/3DzaGK

2 Luccioni, S. (2023, April 12). The mounting human and environmental costs of generative AI. Ars Technica. https://clck.ru/3DzaKM

3 AI Now Institute. (2023). Algorithmic Accountability: Moving Beyond Audits. https://clck.ru/3DzaLM

4 Meredith, S. (2023, December 6). A 'thirsty' generative AI boom poses a growing problem for Big Tech. CNBC. https://clck.ru/3DzaLy ; Microsoft (2022). 2022 Environmental Sustainability Report. https://clck.ru/3DzaLy

5 Там же.

Однако главным ограничивающим фактором станут, вероятно, требования к хранению данных (Susskind, 2020). Объем данных, генерируемых во всем мире, растет экспоненциально, удваиваясь примерно каждые два года. Нынешние технологии хранения данных, такие как жесткие диски, приближаются к своим физических пределам с точки зрения миниатюризации и емкости[6].

Важно отметить, что эти характеристики постоянно меняются по мере развития технологий. Исследователи активно разрабатывают более энергоэффективные модели искусственного интеллекта, водосберегающие системы охлаждения для центров обработки данных и новые способы хранения данных с большей емкостью (Chen, 2016).

Предсказать, когда именно возможности для хранения данных будут исчерпаны, довольно сложно. Рост объема данных происходит по экспоненте, но и технологии хранения постоянно развиваются. Однако можно с уверенностью сказать, что в ближайшем будущем физическое пространство всей планеты для хранения данных не понадобится. Мы становимся свидетелями гонки между экспоненциальным ростом и законом Мура (Theis & Wong, 2017). Объем создаваемых данных действительно растет экспоненциально, удваиваясь примерно каждые два года. Даже если рост замедлится до 20 % в год (сейчас он составляет около 70 %), то в долгосрочной перспективе темп роста все равно будет неустойчивым. Существующая инфраструктура и энергетические ограничения будут осложнять поддержание таких темпов[7]. Однако емкость систем хранения данных также быстро растет, следуя тенденции, аналогичной закону Мура (удвоение плотности транзисторов в интегральных схемах примерно каждые два года). Методы сжатия позволяют значительно сократить физическое пространство, необходимое для хранения информации. Хотя в какой-то момент рост объема данных может превысить емкость хранилища, развитие технологий хранения данных, таких как твердотельные накопители, и совершенствование методов сжатия данных могут решить эту проблему (Chen, 2016). Также приводятся аргументы, что не все данные нужно вечно хранить в этих системах. Значительная часть данных не требует постоянного хранения. Через некоторое время можно удалить блоги, временные файлы и часть развлекательного контента. Эффективное управление данными и определение приоритетных категорий данных могут значительно сократить потребности в системах хранения (Arass & Souissi, 2018). Однако в этом случае предполагаемый сверхинтеллект может опуститься до человеческого уровня. Менее совершенная память влечет за собой несовершенные решения, большее количество ошибок и меньшую надежность: иными словами, человеческую производительность. Совершенно новые, пока еще неизвестные технологии хранения данных могут отсрочить эту неизбежность; исследователи изучают альтернативные решения с гораздо большей емкостью, чем традиционные жесткие диски. К ним относятся такие технологии, как ДНК-хранилища, позволяющие хранить огромные объемы данных на очень компактном пространстве (как это делают все живые организмы в своем геноме). Пока эти технологии находятся на ранних стадиях разработки, но обладают огромным потенциалом для долгосрочного архивирования данных (Goldman et al., 2013). К ним относятся и гологра-

6 Rydning, D., Reinsel, J., & Gantz, J. (2018). The digitization of the world from edge to core. International Data Corporation. https://clck.ru/3DzaNN

7 Там же.

фические хранилища, использующие лазерную технологию для хранения данных в трех измерениях, обеспечивая гораздо более высокую плотность, чем традиционные методы (Lin et al., 2020).

Несмотря на все надежды, исследователь Vopson (2020) убедительно подсчитал, сколько лет потребуется для того, чтобы вся масса Земли была отдана под хранение данных при нескольких сценариях ежегодного роста объемов информации. Его подсчет основан на количестве доступных атомов и не зависит от гипотетических новых технологий и методов управления эффективностью хранения данных. Автор приводит следующие значения: 4500 лет при росте объемов информации на 1 % в год, 918 лет при росте на 5 %, 246 лет при росте на 20 % и около 110 лет при росте на 50 % в год. Земная кора составляет всего 0,7 % от общего объема планеты, и это тот объем, который человечество может, хоть и гипотетически, использовать для хранения информации. Таким образом, у нас осталось менее столетия (скорее всего, 30–50 лет или даже меньше) до информационной катастрофы. В соответствующих исследованиях Института AI Now[8] и Стэндфордского института искусственного интеллекта, ориентированного на человека[9], приводятся другие цифры и используются иные подходы, но говорится о тех же тенденциях.

5. Управление как ключ к решению проблем: государственные показатели и доступность данных укрепляют организационные ценности и способствуют устойчивости национальной системы здравоохранения

Мы утверждаем, что недостающее звено, которое позволит адекватно преодолеть разрыв между традиционной практикой здравоохранения и подходом к реагированию на пандемии с использованием искусственного интеллекта, – это эффективное управление. Только государственные меры, соответствующие принципам надлежащего управления, могут стать основой для интеграции искусственного интеллекта с более традиционными методами.

В работе Correia с соавторами (2020a) были рассмотрены традиционные меры, лежащие в основе надежной национальной системы здравоохранения во время пандемий. В частности, авторы рассматривают локдауны, отслеживание контактов и кампании по вакцинации. Эти меры могут быть реализованы для замедления распространения вирусов, защиты уязвимых групп населения и достижения коллективного иммунитета. Они воплощают в себе приоритетность общественного здоровья и демонстрируют, что правительство несет ответственность перед своими гражданами. Второй важный момент, который подчеркивают авторы, заключается в том, что данные играют решающую роль в мониторинге уровня заражения, отслеживании распределения ресурсов и понимании результатов лечения пациентов. Именно это позволяет принимать решения, что, в свою очередь, укрепляет ценность доказательной практики и в конечном итоге способствует эффективному использованию ресурсов в системе здравоохранения.

---

8 AI Now Institute. (2023). Algorithmic Accountability: Moving Beyond Audits. https://clck.ru/3DzaQC

9 Stanford Institute for Human-Centered Artificial Intelligence. (2023). Sustainability and AI. https://clck.ru/3DzaRd

Таким образом, появляется возможность достичь устойчивости через эффективность, при этом искусственный интеллект может усилить действие традиционных мер. Хотя традиционные меры по-прежнему важны и, вероятно, всегда будут важны, искусственный интеллект дает возможность значительного повышения их эффективности и усиления устойчивости национальных систем здравоохранения. Одним из непосредственных воплощений этой идеи может стать использование моделей искусственного интеллекта для анализа исторических данных, выявления закономерностей и прогнозирования возникновения или распространения вспышек заболеваний, эпидемий и пандемий. Это позволит принимать упреждающие меры в системе здравоохранения, включая раннее оповещение, создание запасов жизненно важных материалов и стратегическое развертывание ресурсов. В частности, оптимизация распределения ресурсов с помощью алгоритмов искусственного интеллекта может быть легко использована в реальном времени при анализе данных об уровне инфекций, пропускной способности больниц и наличии материальных ресурсов. Это даст возможность динамически распределять медицинский персонал, оборудование и критически важные материалы в районах, испытывающих наибольшую нагрузку (Correia et al., 2021, 2022), и, следовательно, обеспечивать эффективное управление ресурсами. Более продвинутые и, соответственно, сложные варианты применения предусматривают разработку персонализированных планов лечения. Это потребует анализа индивидуальных особенностей пациента, таких как история болезни и генетические данные. Искусственный интеллект потенциально может помочь медицинским работникам в разработке планов лечения для достижения максимальной эффективности, способствуя ускорению сроков выздоровления, улучшению результатов лечения пациентов и снижению нагрузки на систему здравоохранения (Jiang et al., 2017).

Таким образом, становится очевидным, что эффективность управления в борьбе с пандемией (независимо от того, используется искусственный интеллект или нет) зависит от наличия высококачественных, всеобъемлющих данных, собранных с помощью традиционных мер и методов, таких как отслеживание контактов и истории болезней пациентов (Wu et al., 2022). Однако при правильной организации управления должна учитываться также проблема конфиденциальности данных. Это касается сбора и использования данных о пациентах, в том числе для обучения искусственного интеллекта. Необходимо также обеспечить анонимность данных и надежность протоколов информационной безопасности для поддержания доверия со стороны общества (Smidt & Jokonya, 2021).

Эффективное использование искусственного интеллекта в здравоохранении требует беспрепятственного обмена данными между различными медицинскими учреждениями и совместимости между операционными системами (O'Reilly-Shah et al., 2020). Первостепенное значение имеет наличие стандартизированных форматов данных и безопасных каналов связи для обмена данными (Sass et al., 2020).

В заключение следует отметить, что для создания устойчивых систем здравоохранения можно реализовать симбиотические отношения. Традиционные меры общественного здравоохранения, доступность данных и искусственный интеллект не являются отдельными сущностями, но могут стать взаимосвязанными элементами в борьбе с пандемиями. Существующая инфраструктура данных и опыт применения традиционных мер создают благоприятную почву для интеграции (Baclic et al., 2020). Используя возможности искусственного интеллекта в сочетании с устоявшейся практикой, национальные системы здравоохранения могут добиться

большей эффективности, персонализировать подходы к лечению и в конечном итоге обеспечить свою долгосрочную устойчивость перед лицом будущих событий (Gunasekeran et al., 2021). Другими словами, надежные методы управления и твердые организационные принципы должны стать залогом для будущей интеграции искусственного интеллекта в эту важнейшую область.

6. Управление как ключ к решению проблем: управление укрепляет организационные ценности и способствует эффективности антикризисных мер

Приведенное выше утверждение имеет огромное значение в контексте применения искусственного интеллекта в борьбе с пандемиями. Это связано с тем, что эффективные методы управления обеспечивают основу и руководящие принципы для ответственного и этичного использования искусственного интеллекта в управлении кризисами, ярким примером которых являются пандемии.

Управление предполагает открытую коммуникацию и ответственность лиц, принимающих решения, за свои действия. Это крайне важно для укрепления доверия общественности к решениям на базе искусственного интеллекта, используемым во время пандемий, например, приложениям для отслеживания контактов. Чтобы избежать опасений общественности, необходимо четко объяснять, как используется искусственный интеллект и как обеспечивается конфиденциальность данных (Galetsi et al., 2022). Эффективное управление также способствует сотрудничеству, включая обмен данными, и координации действий различных заинтересованных сторон, в том числе помогает при распределении ресурсов, разработке вакцин и стратегий коммуникации. Такое сотрудничество и взаимодействие охватывают государственные органы, медицинские учреждения, исследовательские организации и частный сектор (Bulled, 2023).

Эффективное управление воплощается в конкретных организационных принципах, которые должны определять развитие искусственного интеллекта и его использование в условиях пандемии. При правильном применении оно способствует равенству и справедливости, адекватному распределению ресурсов и преодолению цифрового разрыва. Это, в свою очередь, может гарантировать, что инструменты искусственного интеллекта не будут усугублять существующее социальное неравенство (Margetts, 2022). Например, приложения для отслеживания контактов с помощью искусственного интеллекта должны быть доступны для всех групп населения и не должны несправедливо воздействовать на определенные группы. Управление также может стать определяющим фактором в создании надежных протоколов конфиденциальности и безопасности данных. Это способствует защите информации граждан, обеспечивая при этом ответственный сбор данных и их использование для разработки искусственного интеллекта при ликвидации последствий пандемии. Во время пандемии крайне важно найти баланс между инновационными решениями и безопасностью данных (Zhang et al., 2022). Кроме того, надлежащее управление необходимо при принятии решений на основе фактических данных, так как оно создает традицию опоры на научные данные и доказательства для обоснования решений. Это прекрасно согласуется с основным принципом искусственного интеллекта, который использует анализ данных для выработки выводов и рекомендаций, в том числе для руководителей системы здравоохранения (Rubin et al., 2021).

Добавим, что эффективное и устойчивое реагирование в условиях пандемии требует перспективного подхода и долгосрочного планирования. Эффективные методы управления способствуют устойчивости антикризисного управления в нескольких направлениях. Задача руководства – обеспечить долгосрочные инвестиции в инфраструктуру и поддержание аппаратного и программного обеспечения, а также экспертных знаний, необходимых для разработки и внедрения искусственного интеллекта в здравоохранении. Это включает в себя инвестиции в научные исследования и разработки, программы подготовки специалистов по искусственному интеллекту в медицинских учреждениях и создание надежных систем управления данными (Balog-Way & McComas, 2022). Необходимо также разрабатывать перспективные стратегии, создавать гибкие механизмы, способные адаптироваться к меняющимся угрозам и пандемиям с новыми характеристиками. Это гарантирует, что искусственный интеллект останется актуальным и полезным для решения будущих проблем здравоохранения. Например, алгоритмы искусственного интеллекта для прогнозирования пандемий должны быть адаптируемыми для работы с новыми штаммами и вариациями вирусов. Эффективное управление также способно формировать и укреплять доверие общества к государственным учреждениям и использованию ими искусственного интеллекта во время пандемии (Romano et al., 2021). Такое доверие способствует сотрудничеству в области инициатив искусственного интеллекта, таких как приложения для отслеживания контактов и симптомов.

В работе Correia с соавторами (2020b) исследовались принципы, которые создают прочную основу для решений в области борьбы с пандемиями. Способствуя сотрудничеству, ставя во главу угла этические ценности и обеспечивая долгосрочную устойчивость, практика управления открывает путь к тому, чтобы стать мощным оружием в арсенале борьбы с пандемиями и построить более устойчивое будущее для общественного здравоохранения. Авторы предлагают модель, включающую шесть измерений и восемь гипотез, которая уже прошла проверку в конкретных обстоятельствах. Модель представлена на рис. 1.

Рис. 1. Кризисное управление: структурная модель в условиях пандемии COVID-19
(Correia et al., 2020b)

Можно утверждать, что включение этих исходных данных (моделей, показателей и связей между показателями), человеческих факторов является тем звеном, которое необходимо для создания благоприятной среды с помощью эффективного управления, чтобы искусственный интеллект использовался ответственно и этично, одновременно повышая его эффективность в таких сферах, как прогнозирование, подготовка и предупреждение вспышек заболеваний, прогнозирование и подготовка реакции людей на меры общественного здравоохранения, оптимизация распределения стратегических ресурсов в режиме реального времени на основе показателей инфицирования, разработка целевых, персонализированных мер для лиц с высоким риском, а также отслеживание, локализация, изоляция и ограничение распространения патогенов.

Взаимосвязь между эффективным управлением, моделями кризисного управления и решениями искусственного интеллекта, а также синергетический эффект от их применения обладают огромным потенциалом для повышения готовности к будущим пандемиям и реагирования на них, что в конечном итоге позволит спасти жизни людей и обеспечить более устойчивое будущее для здравоохранения во всем мире.

7. Критические положения

Искусственный интеллект представляет собой одну из величайших технологических инноваций современной эпохи, способную кардинально изменить общество во многих аспектах (Bostrom, 2014). Однако эта трансформация также несет с собой серьезные вызовы и опасения по поводу хрупкости современных человеческих обществ.

Цифровое неравенство представляет собой насущную проблему, поскольку интеграция искусственного интеллекта в различных областях может увеличить социально-экономические разрывы, усиливая неравенство между людьми, имеющими доступ к технологическим достижениям и умеющими их использовать, и теми, кто не имеет таких ресурсов (Eubanks, 2018). Это явление способно усилить уже существующее неравенство и одновременно породить новые проявления цифрового отчуждения.

Появление автоматизации, основанной на искусственном интеллекте, также создает значительный риск вытеснения многих традиционных профессий, особенно тех, которые характеризуются рутинными и предсказуемыми действиями. Такой переход может привести к массовой безработице и вызвать глубокий экзистенциальный кризис, основанный на вытеснении человека технологическими инновациями. Сектор здравоохранения, видимо, не является исключением в отношении этой опасности (Hazarika, 2020).

Более того, алгоритмы искусственного интеллекта, особенно в таких важных сферах, как правосудие, здравоохранение и финансы, подвержены манипуляциям и предвзятости, что создает риск несправедливых и вредных последствий, особенно для маргинализированных и уязвимых сообществ (Obermeyer, 2019).

Опасения по поводу конфиденциальности и безопасности данных усиливаются в связи с обширной практикой сбора и анализа данных, на основе которых работают алгоритмы искусственного интеллекта. Отсутствие прозрачности и контроля использования данных представляет собой предсказуемую и значительную угрозу общественному доверию к технологиям, государственной политике и государственным институтам (Larsson & Heintz, 2020).

Кроме того, во всем мире люди все чаще сталкиваются с поляризацией и дезинформацией. Это проявляется в злоупотреблении цифровыми платформами, управляемыми искусственным интеллектом, и может подорвать социальную сплоченность и доверие к демократическим институтам, приводя к все более фрагментированному и расколотому обществу (Kavanagh & Rich, 2018).

Нельзя игнорировать и потенциальные опасности, связанные с чрезмерной зависимостью от технологий. Чем больше человечество зависит от искусственного интеллекта в принятии решений и выполнении задач, тем слабее становится способность человека функционировать самостоятельно (Bostrom, 2014). Такая уязвимость к сбоям и системным отказам в работе искусственного интеллекта может иметь разрушительные последствия.

Кроме того, искусственный интеллект все больше вторгается в нашу жизнь, или, выражаясь более техническим языком, все заметнее становится снижение автономии и самостоятельности человека (Ettlinger, 2022). Растущая интеграция искусственного интеллекта в жизнь людей может привести к разрушению человеческой автономии и самостоятельности, поскольку мы все чаще оставляем принятие важных решений на усмотрение автоматизированных систем. Это поднимает вопросы о том, кто контролирует технологии и кому можно доверить принятие решений, влияющих на нашу жизнь.

Наконец, этот первоначальный, поверхностный анализ проблем должен охватывать не только сиюминутные опасения, но и экзистенциальные риски, о которых часто говорят. Они представляют собой долгосрочные опасения по поводу развития искусственного интеллекта, включая распространенные сценарии искусственных сверхразумов, не контролируемых человеком и угрожающих выживанию человечества (Bostrom, 2014).

По сути, слияние искусственного интеллекта с хрупкой природой современных человеческих обществ заставляет глубоко задуматься над вопросами этики, управления, справедливости и человеческих принципов. Для решения этих вопросов жизненно важен комплексный подход, чтобы при разработке и внедрении искусственного интеллекта во главу угла ставились благосостояние людей и устойчивое развитие (Jobin et al., 2019).

Попытаемся, однако, чуть глубже взглянуть на осознанное стремление человечества использовать искусственный интеллект ответственным, продуктивным и безопасным образом.

При правильной нагрузке системы искусственного интеллекта оказываются весьма хрупкими и уязвимыми. Это может проявляться по-разному, в зависимости от контекста и характера систем искусственного интеллекта. Например, возможны враждебные атаки, связанные с намеренным манипулированием входными данными этих систем таким образом, чтобы заставить их совершать ошибки или выдавать неверные результаты. Такие атаки могут использовать уязвимости алгоритмов искусственного интеллекта, например, нейронных сетей глубокого обучения, приводя к неожиданным и потенциально опасным действиям (Ruan et al., 2021). Еще один подобный пример, рассматриваемый с другой точки зрения, – это использование нерепрезентативных данных для обучения моделей искусственного интеллекта, что также приводит к неверным решениям или прогнозам. При определенных условиях может усиливаться предвзятость, например, когда система искусственного интеллекта сталкивается с новыми данными, которые значительно отличаются от тех,

на которых ее обучали. В результате ИИ может оказаться неспособным к эффективному обобщению, что приведет к нестабильности его работы (Navigli et al., 2023). Другой пример – так называемое катастрофическое забывание: некоторые системы искусственного интеллекта, в частности основанные на искусственных нейронных сетях, могут демонстрировать катастрофическое забывание при получении новых данных. Это происходит, когда система искусственного интеллекта забывает ранее изученную информацию по мере поступления новой, что приводит к снижению производительности или точности с течением времени. Такая уязвимость ограничивает способность системы адаптироваться к изменяющимся условиям или задачам (Kirkpatrick et al., 2017). Еще один пример – хрупкость модели, т. е. неустойчивость системы искусственного интеллекта к небольшим изменениям входных данных или параметров. Например, небольшие возмущения входных изображений не позволяют системе распознавания образов правильно классифицировать объекты. Это может привести к опасным последствиям в таких областях, как автономные транспортные средства или медицинская диагностика (Chen et al., 2020). Последний пример уязвимости искусственного интеллекта – это присущее ему свойство сложности системы. По мере того как системы искусственного интеллекта становятся более сложными и взаимосвязанными, они все более подвержены сбоям или отказам отдельных компонентов. Сбой в одной части системы каскадно отражается на других частях, что приводит к общесистемным отказам или поломкам (Chen et al., 2020). Сложность – это обоюдоострый меч, поскольку мощь многих систем обусловлена их сложностью и способностью обрабатывать огромные объемы данных. Однако эта сложность является и их слабостью, поскольку она увеличивает возможности для потенциальных атак и делает систему более недоступной для понимания и защиты. Эта уязвимость подчеркивает первостепенное значение надежности и устойчивости при разработке и развертывании систем искусственного интеллекта. Решение проблемы уязвимости систем искусственного интеллекта требует пристального внимания к процессам разработки, тестирования и валидации, а также постоянного мониторинга и обслуживания таких систем. Это также подчеркивает необходимость прозрачности, подотчетности и соблюдения этических принципов при разработке и внедрении технологий искусственного интеллекта. Решив эти проблемы, отдельные личности, организации и сообщества смогут работать над созданием систем искусственного интеллекта, которые будут более устойчивыми, надежными и заслуживающими доверия в широком спектре приложений. Если же подобные проблемы, возникающие по отдельности или совокупно, не будут решены, это приведет к катастрофическим последствиям в системе здравоохранения в случае эпидемического или пандемического кризиса.

Еще одно противоречие состоит в том, что развитие искусственного интеллекта, даже если оно кажется несомненным, часто нарушается наличием «узких мест» – критических точек, где сбой или нарушение работы может иметь каскадные последствия для всей системы. Эта двойственность, когда сосуществуют прочность и хрупкость, присуща многим сложным системам искусственного интеллекта (Zhou et al., 2024). Например, как мы уже видели, модели искусственного интеллекта часто включают в себя сложные комплексы взаимосвязанных компонентов, таких как слои в глубоких нейронных сетях или узлы в моделях на основе графов. Такая взаимосвязанность повышает надежность системы, обеспечивая избыточность и отказоустойчивость, но она также создает «узкие места», когда отказ или нарушение работы критического

компонента может распространиться по всей сети (Villegas-Ch et al., 2024). Другой пример – возникновение критических зависимостей. В таком качестве могут выступать определенные компоненты приложений искусственного интеллекта, от которых зависит функциональность всей системы. К таким «критическим точкам» относятся определенные слои или узлы нейронных сетей, играющие ключевую роль в обработке информации или принятии решений. Если эти компоненты выйдут из строя или дадут сбой, будет нарушена работа всей системы (Macrae, 2022). Еще одна тенденция – чувствительность систем искусственного интеллекта к входным данным, особенно в таких областях, как распознавание изображений или обработка естественного языка. Небольшие возмущения или ошибочные входные данные в «критической точке» могут привести к значительным изменениям в результатах работы системы. Такая чувствительность подчеркивает уязвимость в отношении определенных типов действий с входными данными (Dhingra & Gupta, 2017). Последний пример, иллюстрирующий опасность «критических точек», – это особенности дизайна, построенного на компромиссе между надежностью и эффективностью. Стратегии, направленные на повышение надежности, такие как добавление избыточности или механизмов исправления ошибок, создают дополнительные «критические точки» или увеличивают стоимость вычислений. И наоборот, оптимизация для повышения эффективности может непреднамеренно увеличить уязвимость системы за счет уменьшения избыточности или отказоустойчивости. Решение этих специфических проблем требует многогранного подхода, включая выявление и смягчение проблемных моментов и повышение устойчивости за счет избыточности и разнообразия (Goodfellow et al., 2016). Понимая этот тонкий баланс, ученые, инженеры и практики могут работать над созданием более устойчивых и надежных технологий искусственного интеллекта.

Сложность систем искусственного интеллекта еще более повышается, когда мы расширяем и детализируем понятие «потеря контроля» – иными словами, когда это понятие действительно начинает отражать все сложности и проблемы, связанные с разработкой и внедрением технологий искусственного интеллекта. Одно из таких проявлений связано с автономностью и принятием решений (Wallach & Allen, 2008). По мере того как системы искусственного интеллекта становятся все более автономными и способными принимать решения без непосредственного вмешательства человека, возникает опасность утраты контроля над результатами этих решений. Это особенно актуально для высокорисковых областей, таких как автономные транспортные средства или медицинские приборы, где действия систем искусственного интеллекта могут иметь угрожающие жизни последствия в реальном мире. Еще одно проявление указанного свойства – это непрозрачность, присущая системам искусственного интеллекта, особенно основанных на глубоком обучении и нейронных сетях, что затрудняет понимание и интерпретацию их внутренней работы человеком. Отсутствие прозрачности приводит к потере контроля над тем, как системы ИИ принимают свои решения, что вызывает опасения по поводу подотчетности и доверия (Chiao, 2019). Еще одно проявление заключается в том, что системы искусственного интеллекта могут демонстрировать эмерджентное поведение, когда сложные модели или модели поведения возникают в результате взаимодействия простых компонентов. Такое эмерджентное поведение трудно предсказать или контролировать, что приводит к неопределенности в отношении поведения систем в новых или непредвиденных ситуациях. Это само по себе может привести к непредсказуемым

последствиям, поскольку действия или решения функций искусственного интеллекта приводят к результатам, которые не были предусмотрены или запланированы их создателями. Причина может лежать в неожиданных взаимодействиях с окружающей средой или других факторах (Bostrom, 2014). И последнее, но не менее важное: необходимо учитывать этические и социальные последствия. Потеря контроля над технологиями искусственного интеллекта может иметь и более широкие этические и общественные последствия, такие как влияние искусственного интеллекта на занятость, частную жизнь, безопасность и неравенство, о чем мы будем говорить далее (Thomsen, 2019). Эти проблемы подчеркивают необходимость ответственного развития искусственного интеллекта и управления им. Важно обеспечить внедрение технологий таким образом, чтобы они приносили пользу всему обществу, а не только олигархии, крупным технологическим компаниям и правящей элите. Решение этих проблем требует целостного подхода, включающего технические, этические и нормативные аспекты. Сюда относятся и обеспечение прозрачности и подотчетности систем искусственного интеллекта, а также постоянный диалог и сотрудничество между заинтересованными сторонами для снижения рисков и максимизации выгоды.

Еще одна сложность возникает в аспекте предпосылки надежности, особенно в периоды напряженности или неопределенности, когда она требует срочной переоценки. Одним из примеров неверной предпосылки является взаимосвязанность. Системы искусственного интеллекта представляют собой сложный набор взаимосвязанных компонентов, каждый из которых вносит свой вклад в общую функциональность. При возникновении напряженности или неожиданных условий, таких как атаки противника, аномалии данных или изменения окружающей среды, сложность этих систем увеличивает вероятность сбоя. Отсюда необходимость более тонкого понимания надежности, выходящей за рамки традиционных показателей (Macrae, 2022). Еще один пример – непредсказуемость. Эмерджентное поведение систем ИИ приводит к непредсказуемости их реакции на стрессовые факторы. Даже незначительные возмущения или вариации входных данных могут привести к неожиданным результатам, что подчеркивает сложность обеспечения надежности в различных условиях. Это говорит о важности тестирования на устойчивость и планирования различных сценариев для выявления потенциальных точек отказа и смягчения возможных последствий (Bostrom, 2014). Именно эти опасения были показаны выше. Еще один пример этого класса явлений связан с адаптивными и развивающимися средами, поскольку системы искусственного интеллекта работают в динамичной и постоянно меняющейся обстановке, где условия могут меняться быстро и непредсказуемо. В такой ситуации понятие надежности как статичного свойства становится неадекватным. Вместо этого надежность следует рассматривать как динамическое свойство, которое адаптируется к изменяющимся обстоятельствам, требуя постоянного мониторинга, адаптации и механизмов обратной связи (Sundar, 2020). Последний пример посвящен тесной взаимосвязи между этими типами систем и человеко-машинным взаимодействием. Люди-операторы играют важнейшую роль в мониторинге производительности системы, интерпретации результатов и вмешательстве в случае необходимости. Однако в условиях стресса или высокого напряжения операторы-люди могут быть склонны к ошибкам или когнитивным предубеждениям, что влияет на надежность систем (Hoff & Bashir, 2015). В свете этих проблем переосмысление предпосылок надежности в системах ИИ требует более адаптивных,

устойчивых и учитывающих контекст подходов. Среди них – соблюдение принципов количественной оценки неопределенности, надежности решений и человекоориентированного проектирования при разработке и внедрении моделей и приложений искусственного интеллекта. Приняв на вооружение более широкое понимание надежности и заблаговременно устранив факторы, способствующие сбоям, человечество сможет создать более надежные и безотказные технологии искусственного интеллекта. Первостепенной задачей должна стать подготовка плана действий в непредвиденных обстоятельствах без участия искусственного интеллекта, чтобы общество могло продолжать функционировать в случае технологического кризиса или коллапса. Если правосудие «дематериализуется», сохранится ли система правосудия в большинстве развитых стран, если не во всех, если завтра Интернет выйдет из строя? Хотим ли мы идти на риск, который может привести к остановке или полному краху общественных отношений?

Еще более глубокая проблема, еще одно препятствие, которое необходимо преодолеть, – это переход от предпосылки надежности к предпосылке риска в отношении искусственного интеллекта. Это равносильно переходу от неподвижности к быстрому реагированию на меняющиеся обстоятельства. Один из примеров – понимание риска. Надежность часто ассоциируется с понятием детерминированности результатов и предсказуемости поведения. Однако в сложных и динамичных условиях, с которыми сталкиваются системы искусственного интеллекта, полная надежность может оказаться недостижимой. Если признать это, то акцент смещается на понимание и управление рисками; отсюда аспекты вероятности и влияния неблагоприятных событий или неопределенностей (Bigham et al., 2019). Принятие риска подразумевает признание неопределенности, присущей системам искусственного интеллекта, и использование адаптивных стратегий для ее преодоления. Вместо того чтобы стремиться к абсолютной надежности, системы искусственного интеллекта должны быть спроектированы таким образом, чтобы быть устойчивыми и быстро реагировать на изменяющиеся обстоятельства. Это подразумевает механизмы мониторинга в реальном времени, динамической корректировки и обучения на опыте (Syed et al., 2023). Такой способ реагирования на изменяющиеся обстоятельства требует от этих приложений быстроты и гибкости, включая способность быстро оценивать риски, выявлять возможности и соответствующим образом адаптировать поведение или стратегии принятия решений. Гибкие системы искусственного интеллекта будут обладать способностью все более динамично распределять ресурсы, расставлять приоритеты и адаптироваться к новой информации или целям по мере их появления. Переход от установки на надежность к установке на риск требует разработки надежных принципов управления рисками. Эти принципы должны обеспечивать систематический подход к выявлению, оценке, снижению и мониторингу рисков на протяжении всего жизненного цикла использования искусственного интеллекта. Проактивно управляя рисками, организации могут повысить устойчивость и снизить вероятность неблагоприятных исходов (Jobin et al., 2019). Несомненно, что использование искусственного интеллекта с учетом рисков должно ориентироваться на непрерывное обучение и совершенствование, используя петли обратной связи, эксперименты и данные для итеративного повышения эффективности и адаптации к меняющимся проблемам. Такой итеративный подход позволит системам искусственного интеллекта со временем совершенствовать свои стратегии и становиться более эффективными в управлении рисками. Последний фрагмент

этой головоломки появится в результате признания ограниченности возможностей систем ИИ в сложных и неопределенных ситуациях и, как следствие, усиления акцента на подходе «человек в контуре» (Russell & Norvig, 2021). Благодаря интеграции человеческих суждений, опыта и надзора системы искусственного интеллекта смогут более адекватно дополнять процесс принятия решений человеком, снижать риски и повышать общую эффективность системы (Parasuraman & Riley, 1997). В целом переход от парадигмы надежности к парадигме риска отражает более широкое признание неопределенности и сложности, присущих реальным приложениям. Принимая риски и развивая гибкость в реагировании на изменяющиеся обстоятельства, модели искусственного интеллекта могут лучше ориентироваться в ситуации неопределенности, адаптироваться к изменяющимся задачам и в конечном итоге демонстрировать большую ценность и влияние в различных областях, к которым не в последнюю очередь относится здравоохранение.

Следующий уровень проблемы состоит в том, что искусственный интеллект может маскировать свои слабые стороны под сильные, особенно когда речь идет об определенных типах моделей или алгоритмов машинного обучения. Самым вопиющим примером является дисбаланс между обобщением и чрезмерной подгонкой, когда модель учится хорошо работать на обучающих данных, но не может обобщить их на новые, неизвестные данные (Igual & Seguí, 2024). Это создает иллюзию надежности, поскольку модель кажется исключительно хорошо работающей на данных, на которых она была обучена. Однако при изучении новых данных слабые стороны модели становятся очевидными, поскольку она не может делать точные предсказания. Так, система визуального распознавания легко учится определять галстуки на фотографиях и ассоциировать их с мужчинами, если ее обучить на наборе данных о высокопоставленных лицах с Уолл-стрит. Это происходит потому, что модели искусственного интеллекта нацелены обобщать шаблоны из обучающих данных и делать предсказания по неизвестным данным. Способность к обобщению необходима, однако чрезмерная зависимость от конкретных паттернов в обучающих данных может привести к подгонке, когда модель не может эффективно обобщать. Понимание баланса между обобщением и чрезмерной подгонкой имеет решающее значение для обеспечения надежности. Тщательное тестирование систем искусственного интеллекта на различных наборах данных, внимательный анализ процессов принятия решений и устранение предвзятости и уязвимостей позволяют пользователям выявлять и устранять слабые стороны, замаскированные под сильные, что приводит к созданию более надежных и заслуживающих доверия систем.

По мере углубления анализа приходит понимание того, что искусственный интеллект культивирует нестабильность. Коллектив, привыкший к тому, что все работает и будет работать без перебоев, а блокировки либо случайны, либо незначительны по своему воздействию, несомненно, гораздо менее подготовлен к тому, что эти принципы окажутся под угрозой. Зависимость от искусственного интеллекта все больше внедряется в различные аспекты жизни общества, и растет зависимость от его функциональности. Отдельные лица, организации, правительства и наднациональные институты (такие как Организация Объединенных Наций и Всемирная организация здравоохранения) все больше полагаются на искусственный интеллект в принятии решений, автоматизации и оптимизации процессов (Bostrom, 2014). Однако такая зависимость может привести к нестабильности, если эти функции будут давать сбои или нарушаться. Повсеместное внедрение решений на основе

искусственного интеллекта формирует коллективные ожидания непрерывности и бесперебойности работы. Когда эти решения функционируют так, как ожидается, они укрепляют представление о том, что риски минимальны. Однако это может привести к самоуспокоенности и уязвимости, если системы столкнутся с неожиданными проблемами или сбоями (Parasuraman et al., 2000). Из этого следует, что, когда приложения искусственного интеллекта выходят из строя или блокируются, последствия будут значительными, особенно если на них полагаются при выполнении критически важных задач или услуг. Перебои в технологических процессах могут разрушить цепочки поставок, финансовые рынки, коммуникационные сети и другие важнейшие функции и системы (например, атомные электростанции), что приведет к экономическим потерям, социальным беспорядкам и даже угрозе безопасности. Для повышения устойчивости и адаптивности перед лицом этой потенциальной нестабильности необходимы проактивные меры по прогнозированию и снижению рисков, о чем уже говорилось выше. Это может включать диверсификацию технологических зависимостей, создание избыточности в критически важных системах и разработку человекоориентированных подходов к принятию решений и решению проблем (Bigham et al., 2019; Jobin et al., 2019). Таким образом, технологии искусственного интеллекта также создают проблемы, связанные со стабильностью и устойчивостью. Признавая потенциальную нестабильность, присущую этим системам, и принимая упреждающие меры по устранению рисков, заинтересованные стороны могут лучше ориентироваться в сложностях мира, управляемого искусственным интеллектом, и создавать более надежные и устойчивые системы.

Наконец, добравшись до самой глубины – до центра Вселенной и ее самого холодного места, по Аристотелю, или центра Земли и Ада, по Данте, – мы должны рассмотреть искусственный интеллект в свете того, что можно назвать люциферианской семиотикой, путешествием в символические или метафорические последствия искусственного интеллекта. В различных мифологиях и системах верований Люцифер (люциферианская символика) часто ассоциируется с темами бунтарства, просвещения и стремления к знаниям. Люцифер часто изображается как носитель света (Hanegraaff, 2013). Таким образом, термин «люциферианец» может означать стремление к знаниям или силе, которое бросает вызов устоявшимся нормам или структурам власти. Семиотика относится к изучению знаков и символов и их интерпретации. В контексте искусственного интеллекта семиотика охватывает символические значения, связанные с искусственным интеллектом, включая понятия разума, автономии и контроля (Binder, 2024). Искусственный интеллект часто воспринимается как символ силы и возможностей, учитывая его способность обрабатывать огромные объемы данных, принимать сложные решения и эффективно автоматизировать задачи. Такое представление о могуществе подкрепляется впечатляющими деяниями ИИ в различных областях. Однако, как было показано выше, объекты или сущности, которые кажутся сильными, на самом деле могут обладать уязвимостями или слабостями, которые не сразу бросаются в глаза. Такое изменение ожиданий на противоположное можно рассматривать как проявление люциферианской символики, когда стремление к знаниям или власти приводит к переоценке устоявшихся истин или предположений. Модели и системы искусственного интеллекта, несмотря на их кажущуюся мощь, в определенных контекстах демонстрируют уязвимость или ограниченность. Эти слабости могут стать более заметными с течением времени, когда технологии искусственного интеллекта будут

подвергаться тщательному изучению, экспериментам и внедрению в реальный мир. Исследование люциферианской семиотики поднимает более широкие этические и философские вопросы (Bostrom, 2014) о природе власти, знания и контроля в эпоху искусственного интеллекта. Это побуждает задуматься о непредвиденных последствиях технологического прогресса и необходимости ответственного отношения к любым технологиям. Таким образом, люциферианская семиотика, примененная к искусственному интеллекту, предлагает нам рассмотреть символические значения и последствия искусственного интеллекта, включая то, как восприятие силы и власти может быть подорвано или поставлено под сомнение более глубоким изучением и пониманием. Это подчеркивает важность критического исследования и этических размышлений при изучении сложностей искусственного интеллекта и его влияния на общество, государственную политику и политические системы.

Каковы же перспективы использования искусственного интеллекта в борьбе с пандемиями с учетом вышесказанного? Возможно, лучший вариант действий для человечества – продолжать полагаться на человеческий фактор. Люди совершают больше ошибок, в этом нет сомнений. Но большинство этих ошибок мелкие и незначительные. Они могут привести к отдельным трагедиям, но не к глобальным. Модели искусственного интеллекта для борьбы со вспышками заболеваний, эпидемиями и пандемиями, а также другие медицинские приложения, основанные на искусственном интеллекте, могут быть практически безошибочными. Но одна ошибка может погубить всех.

8. Искусственный интеллект и фундаментальные права

Влияние ИИ на основные права настолько актуально, что не осталось незамеченным законодателем. Статья 27 Закона об ИИ требует, чтобы системы с высоким уровнем риска проходили оценку в отношении их влияния на основные права. Основная цель такой оценки – выявить и смягчить потенциальные угрозы, которые эти системы могут представлять для основных прав человека. Это особенно важно, когда речь идет о системах ИИ с высоким уровнем риска, которые способны существенно повлиять на жизнь и благосостояние людей. В целом можно сказать, что, осознавая негативные последствия ИИ, человечество решило не отказываться от него, а, напротив, воспользоваться его положительными свойствами, классифицировав системы ИИ по степени риска и осуществляя их предварительный, сопутствующий и последующий контроль.

Существует несколько направлений взаимосвязей между ИИ и основными правами. В частности, это влияние, которое ИИ может оказать на осуществление и, напротив, на нарушение основных прав. В любом случае есть основания полагать, что, как отмечает Агентство Европейского союза по основным правам[10], даже в ограниченном контексте отсутствие большого объема эмпирических данных по широкому спектру прав, связанных с ИИ, затрудняет задачу обеспечения необходимых гарантий для того, чтобы использование ИИ эффективно соответствовало основным правам.

[10] FRA – European Union Agency for Fundamental Rights, Getting the future right – Artificial intelligence and fundamental rights – Report, Publications Office of the European Union, 2020.

Главный аргумент в пользу использования ИИ – его эффективность (Pedro, 2023). Что касается проблем, то основное беспокойство вызывает нарушение фундаментальных прав. Так, среди основных прав, которым потенциально может навредить ИИ, выделяют право на защиту персональных данных (Gómez Abeja, 2022) и право на недискриминацию (Gómez Abeja, 2022), право на эффективную судебную защиту (Shaelou & Razmetaeva, 2023), право на свободу информации, избирательное право и право на доступ к публичной информации (Gómez Abeja, 2022).

Возвращаясь к работе Агентства Европейского союза по основным правам[11], следует отметить, что использование ИИ может оказывать влияние на основные права, вызывая необходимость гарантировать недискриминационное использование ИИ (право на недискриминацию); требование законной обработки данных (право на защиту персональных данных); возможность подачи жалоб на решения, основанные на ИИ, и подачи апелляций (право на эффективные средства правовой защиты и беспристрастный суд).

Наконец, следует также подчеркнуть, что связь между ИИ и основными правами может быть более тесной, по крайней мере, в следующих аспектах: нарушение неявных основных прав (Gómez Colomer, 2023), таких как принцип верховенства закона и право на рассмотрение дела судьей-человеком, а также появление «новых» или «обновленных» основных прав (Shaelou & Razmetaeva, 2023), таких как право на забвение (Gómez Abeja, 2022), «право не быть объектом автоматических решений и автоматических действий» в широком смысле (Shaelou & Razmetaeva, 2023); «право влиять на свой цифровой след» (Shaelou & Razmetaeva, 2023), а также новые права, такие как «право не быть объектом манипуляции», «право на нейтральное информирование в Сети» и «право на значимый человеческий контакт», «право не быть объектом измерения, анализа или обучения» (Shaelou & Razmetaeva, 2023).

9. Пандемии и фундаментальные права

Ситуация пандемии, как в случае с COVID-19, потребовала введения публично-правовых режимов исключительности (наряду с режимами нормальности). Это не является чем-то новым (Gomes & Pedro, 2020) – вспомним латинское высказывание «У необходимости нет закона, но она сама устанавливает его для себя». Именно так обосновывались чрезвычайные полномочия в римском праве, которые могли быть использованы в случаях, когда необходимо было справиться с непредвиденной ситуацией, требующей немедленного решения, без возможности отсрочки.

Потребность в правовом режиме исключительности и, соответственно, его мобилизация стали более очевидными в последнее время. Этому в значительной степени способствуют высокорисковая конфигурация современного общества (Beck, 1986) и тот факт, что мы живем в экономически и социально глобализированном мире. Несмотря на физические расстояния, здесь все оказывается близким – так, продолжающийся кризис здравоохранения был вызван вспышкой COVID-19, которая за несколько месяцев распространилась из своего источника (китайский город Ухань) на весь мир (Pedro, 2022).

[11] Там же.

Перед лицом катастроф такого рода публичное право не могло и не может оставаться в стороне. Иными словами, учитывая пагубные последствия, которые общественные бедствия оказывают на salus populi – здоровье народа, становится очевидно, что государство должно использовать все имеющиеся в его распоряжении средства для восстановления нормальной жизни (Alvarez Garcia, 1996). Поэтому, чтобы гарантировать верховенство закона, необходимо предусмотреть режимы, достаточно гибкие для соответствия публичным интересам, находящимся под угрозой, режимы, позволяющие реагировать на общественную необходимость, или, другими словами, публично-правовые режимы исключительности.

В рамках реальной нормативности публичное право руководствуется принципом законности публичных действий, что соответствует условиям правовой нормативности. Проблема возникает, когда реальность временно меняется радикальным образом, создавая ситуации неминуемой или реальной опасности для общества. На такие ситуации нормативное публичное право не может дать адекватного ответа, и идея поддержания демократического верховенства права навязывает необходимость введения в действие исключительных правовых режимов – jus extremae necessitatis, чтобы в кратчайшие сроки восстановить нормальность и вернуть в действие нормативные правовые режимы. Речь идет об альтернативной законности, исключительной законности для исключительной ситуации (Correia, 1987) – о замещающей и временной законности.

Таким образом, как правило, в исключительных ситуациях, в условиях чрезвычайного положения, при соблюдении принципа пропорциональности, действие некоторых основных прав может быть приостановлено. Несмотря на это, следует отметить, что действие не всех основных прав может быть приостановлено, например, право на жизнь, личную неприкосновенность, личную идентичность, гражданскую правоспособность и гражданство, отсутствие обратной силы уголовного закона, право на защиту обвиняемых, свобода совести и религии.

10. Возможные взаимосвязи между искусственным интеллектом и фундаментальными правами в борьбе с пандемиями

В демократических правовых государствах рассмотрение вопроса об использовании ИИ для борьбы с пандемиями обычно связано с соблюдением основных прав. Это требует, с одной стороны, рассмотрения воздействия использования ИИ на определенные основные права с учетом рисков, которые несет в себе каждая конкретная система ИИ, а с другой – того, что контекст пандемии, как это произошло с COVID-19, требует признать законность исключений, когда определенные основные права должны быть ограничены с целью защиты таких ценностей, как общественное здоровье, до восстановления нормальной ситуации.

Заключение

В современном мире борьба с болезнями и пандемиями требует комплексного подхода, объединяющего усилия врачей, медицинских учреждений и различных государств. ИИ представляет собой перспективный инструмент, способный кардинально изменить методы противодействия эпидемиям и пандемиям. Его потенциал заключается в анализе больших данных, прогнозировании вспышек заболеваний,

ускорении разработки лекарств, персонализации лечения и оптимизации распределения ресурсов. Примеры использования ИИ, такие как раннее выявление вспышек через анализ данных из социальных сетей, ускорение поиска лекарственных препаратов и улучшение отслеживания контактов, демонстрируют его значимость в борьбе с глобальными угрозами здоровью.

Однако внедрение ИИ в сферу здравоохранения сопряжено с рядом вызовов. К ним относятся проблемы предвзятости данных, сложность алгоритмов, риски чрезмерной зависимости от технологий и этические дилеммы, связанные с соблюдением фундаментальных прав. Использование ИИ для борьбы с пандемиями требует тщательного баланса между инновациями, этикой и защитой прав человека, включая право на приватность, свободу и равный доступ к медицинской помощи.

Таким образом, ИИ, несмотря на свои революционные возможности, не является панацеей. Его применение должно сопровождаться критическим анализом потенциальных рисков и разработкой правовых и этических механизмов, которые обеспечат безопасное и справедливое использование технологий. Только при условии учета этих аспектов ИИ сможет стать эффективным инструментом в борьбе с болезнями, не ставя под угрозу фундаментальные права и свободы человека.

Список литературы

Arass, M., & Souissi, N. (2018). Data lifecycle: from big data to SmartData. In *2018 IEEE 5th International Congress on Information Science and Technology* (pp. 80–87). IEEE. https://doi.org/10.1109/CIST.2018.8596547

Alvarez Garcia, V. (1996). *El concepto de necesidad en derecho público* (1st ed.). Madrid: Civitas. (In Spanish).

Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Baclic, O., Tunis, M., Young, K., Doan, C., Swerdfeger, H., & Schonfeld, J. (2020). Challenges and opportunities for public health made possible by advances in natural language processing. *Canada Communicable Disease Report*, *46*(6), 161–168. https://doi.org/10.14745/ccdr.v46i06a02

Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: transforming the practice of medicine. *Future Healthcare Journal*, *8*(2), e188-e194. https://doi.org/10.7861/fhj.2021-0095

Beck, U. (1986). *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp Verlag.

Balog-Way, D., & McComas, K. (2022). COVID-19: Reflections on trust, tradeoffs, and preparedness. In *COVID-19* (pp. 6–16). Routledge.

Bazarkina, D. Y., & Pashentsev, E. N. (2020). Malicious use of artificial intelligence. *Russia in Global Affairs*, *18*(4), 154–177. https://doi.org/10.31278/1810-6374-2020-18-4-154-177

Benke, K., & Benke, G. (2018). Artificial Intelligence and Big Data in Public Health. *International Journal of Environmental Research and Public Health*, *15*(12), 2796. https://doi.org/10.3390/ijerph15122796

Berk, R. A. (1983). An introduction to sample selection bias in sociological data. *American Sociological Review*, *48*(3), 386–398. https://doi.org/10.2307/2095230

Bigham, G., Adamtey, S., Onsarigo, L., & Jha, N. (2019). Artificial Intelligence for Construction Safety: Mitigation of the Risk of Fall. In K. Arai, S. Kapoor, R. Bhatia (Eds.). *Intelligent Systems and Applications*. Springer. https://doi.org/10.1007/978-3-030-01057-7_76

Binder, W. (2024). Technology as (dis-)enchantment. AlphaGo and the meaning-making of artificial intelligence. *Cultural Sociology*, *18*(1), 24–47. https://doi.org/10.1177/17499755221138720

Bisconti, P., Orsitto, D., Fedorczyk, F., Brau, F., Capasso, M., De Marinis, L., ... & Schettini, C. (2023). Maximizing team synergy in AI-related interdisciplinary groups: an interdisciplinary-by-design iterative methodology. *AI & Society*, *38*(4), 1443–1452. https://doi.org/10.1007/s00146-022-01518-8

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

Box, G. (1979). Robustness in the strategy of scientific model building. In R. Launer & G. Wilkinson (Eds.), *Robustness in Statistics* (pp. 201–236). Academic Press. https://doi.org/10.1016/B978-0-12-438150-6.50018-2

Breiman, L. (2001). Statistical Modeling: The Two Cultures (with comments and a rejoinder by the author). *Statistical Science*, *16*(3), 199–231. https://doi.org/10.1214/ss/1009213726

Bulled, N. (2023). "Solidarity:" A failed call to action during the COVID-19 pandemic. *Public Health in Practice*, *5*, 100379. https://doi.org/10.1016/j.puhip.2023.100379

Chen, A. (2016). A review of emerging non-volatile memory (NVM) technologies and applications. *Solid-State Electronics*, *125*, 25–38. https://doi.org/10.1016/j.sse.2016.07.006

Chen, J., Zhang, R., Han, W., Jiang, W., Hu, J., Lu, X., Liu, X., & Zhao, P. (2020). Path Planning for Autonomous Vehicle Based on a Two-Layered Planning Model in Complex Environment. *Journal of Advanced Transportation*, 2020, 6649867. https://doi.org/10.1155/2020/6649867

Chiao, V. (2019). Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context*, *15*(2), 126–139. https://doi.org/10.1017/S1744552319000077

Correia, P., Mendes, I., Pereira, S., & Subtil, I. (2020a). The combat against COVID-19 in Portugal: How state measures and data availability reinforce some organizational values and contribute to the sustainability of the National Health System. *Sustainability*, *12*(18), 7513. https://doi.org/10.3390/su12187513

Correia, P., Mendes, I., Pereira, S., & Subtil, I. (2020b). The combat against COVID-19 in Portugal, Part II: how governance reinforces some organizational values and contributes to the sustainability of crisis management. *Sustainability*, *12*(20), 8715. https://doi.org/10.3390/su12208715

Correia, P., Pereira, S., Mendes, I., & Subtil, I. (2022). COVID-19 Crisis management and the Portuguese regional governance: Citizens perceptions as evidence. *European Journal of Applied Business Management*, *8*(1), 1–12.

Correia, P., Pereira, S., Mendes, I., & Subtil, I. (2021). COVID-19 Crisis management and the Portuguese regional governance: Citizens perceptions as evidence. In *European Consortium for Political Research General Conference* (pp. 1–18). United Kingdom.

Correia, J. M. C. (1987). *Legalidade e autonomia contratual nos contratos administrativos* (pp. 283, 768). Lisboa: Almedina.

DeCamp, M., & Tilburt, J. (2019). Why we cannot trust artificial intelligence in medicine. *The Lancet Digital health*, *1*(8), e390. https://doi.org/10.1016/S2589-7500(19)30197-9

Dhingra, M., & Gupta, N. (2017). Comparative analysis of fault tolerance models and their challenges in cloud computing. *International Journal of Engineering & Technology*, *6*(2), 36–40. https://doi.org/10.14419/ijet.v6i2.7565

Ettlinger, N. (2022). *Algorithms and the Assault on Critical Thought: Digitalized Dilemmas of Automated Governance and Communitarian Practice* (1st ed.). Routledge. https://doi.org/10.4324/9781003109792

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: Picador, St Martin's Press.

Ferguson, N., Cummings, D., Fraser, C., Cajka, J., Cooley, P., & Burke, D. (2006). Strategies for mitigating an influenza pandemic. *Nature*, *442*(7101), 448–452. https://doi.org/10.1038/nature04795

Fetzer, T., & Graeber, T. (2021). Measuring the scientific effectiveness of contact tracing: Evidence from a natural experiment. *Proceedings of the National Academy of Sciences of the United States of America*, *118*(33), e2100814118. https://doi.org/10.1073/pnas.2100814118

Galetsi, P., Katsaliaki, K., & Kumar, S. (2022). The medical and societal impact of big data analytics and artificial intelligence applications in combating pandemics: A review focused on Covid-19. *Social Science & Medicine*, *301*, 114973. https://doi.org/10.1016/j.socscimed.2022.114973

Gianfrancesco, M., Tamang, S., Yazdany, J., & Schmajuk, G. (2018). Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data. *JAMA Internal Medicine*, *178*(11), 1544–1547. https://doi.org/10.1001/jamainternmed.2018.3763

Goldman, N., Bertone, P., Chen, S., Dessimoz, C., LeProust, E. M., Sipos, B., & Birney, E. (2013). Towards practical, high-capacity, low-maintenance information storage in synthesized DNA. *Nature*, *494*(7435), 77–80. https://doi.org/10.1038/nature11875

Gomes, C. A., & Pedro, R. (Coords.). (2020). *Direito administrativo de necessidade e de excepção*. Lisboa: AAFDL.

Gómez Abeja, L. (2022). Inteligencia artificial y derechos fundamentales. In F. H. Llano Alonso (Dir.), J. Garrido Martín & R. Valdivia Jiménez (Coords.), *Inteligencia artificial y filosofía del derecho* (1.ª ed., pp. 91–114, 93). Murcia: Ediciones Laborum. (In Spanish).

Gómez Colomer, J.-L. (2023). *El juez-robot: La independencia judicial en peligro*. Valencia: Tirant lo Blanch. (In Spanish).

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.

Greiner, R., Grove, A., & Kogan, A. (1997). Knowing what doesn't matter: exploiting the omission of irrelevant data. *Artificial Intelligence*, *97*(1–2), 345–380. https://doi.org/10.1016/S0004-3702(97)00048-9

Gunasekeran, D., Tseng, R., Tham, Y., & Wong, T. (2021). Applications of digital health for public health responses to COVID-19: a systematic scoping review of artificial intelligence, telehealth and related technologies. *NPJ Digital Medicine*, *4*(1), 40. https://doi.org/10.1038/s41746-021-00412-9

Gürsoy, E., & Kaya, Y. (2023). An overview of deep learning techniques for COVID-19 detection: methods, challenges, and future works. *Multimedia Systems*, *29*(3), 1603–1627. https://doi.org/10.1007/s00530-023-01083-0

Hanegraaff, W. (2013). *Western Esotericism: A Guide for the Perplexed*. Bloomsbury Publishing.

Halevy, A., Norvig, P., & Pereira, F. (2009). The unreasonable effectiveness of data. *IEEE Intelligent Systems*, 24(2), 8–12. https://doi.org/10.1109/MIS.2009.36

Hazarika, I. (2020). Artificial intelligence: opportunities and implications for the health workforce. *International Health*, *12*(4), 241–245. https://doi.org/10.1093/inthealth/ihaa007

Hoff, K., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434. https://doi.org/10.1177/0018720814547570

Hulten, G. (2018). Building Intelligent Systems: A Guide to Machine Learning Engineering. Apress.

Igual, L., & Seguí, S. (2024). *Supervised learning. In Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications* (pp. 67–97). Springer International Publishing.

Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, *2*(4), 230–243. https://doi.org/10.1136/svn-2017-000101

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*, 389–399. https://doi.org/10.1038/s42256-019-0088-2

Jones, K., Patel, N., Levy, M., Storeygard, A., Balk, D., Gittleman, J., & Daszak, P. (2008). Global trends in emerging infectious diseases. *Nature*, *451*(7181), 990–993. https://doi.org/10.1038/nature06536

Kandlhofer, M., Weixelbraun, P., Menzinger, M., Steinbauer-Wagner, G., & Kemenesi, Á. (2023). Education and Awareness for Artificial Intelligence. In *International Conference on Informatics in Schools: Situation, Evolution, and Perspectives* (pp. 3–12). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-44900-0_1

Kavanagh, J., & Rich, M. (2018). *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. RAND Corporation. https://doi.org/10.7249/RR2314

Kirkpatrick, J., Pascanu, R., Rabinowitz, N., Veness, J., Desjardins, G., Rusu, A. A., ... & Hadsell, R. (2017). Overcoming catastrophic forgetting in neural networks. *Proceedings of the National Academy of Sciences*, *114*(13), 3521–3526. https://doi.org/10.1073/pnas.1611835114

Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. E*uropean Journal of Information Systems*, *31*(3), 388–409. https://doi.org/10.1080/0960085X.2021.1927212

Larsson, S., & Heintz, F. (2020). Transparency in artificial intelligence. *Internet Policy Review*, *9*(2). https://doi.org/10.14763/2020.2.1469

Lin, X., Liu, J., Hao, J., Wang, K., Zhang, Y., Li, H., ... & Tan, X. (2020). Collinear holographic data storage technologies. *Opto-Electronic Advances*, *3*(3), 190004. https://doi.org/10.29026/oea.2020.190004

Little, R. J., & Rubin, D. B. (2019). Statistical analysis with missing data. John Wiley & Sons.

Macrae, C. (2022). Learning from the failure of autonomous and intelligent systems: Accidents, safety, and sociotechnical sources of risk. *Risk Analysis*, *42*(9), 1999–2025. https://doi.org/10.1111/risa.13850

Margetts, H. (2022). Rethinking AI for good governance. *Daedalus*, *151*(2), 360–371. https://doi.org/10.1162/daed_a_01922

Matsuzaka, Y., & Yashiro, R. (2022). Applications of Deep Learning for Drug Discovery Systems with BigData. *BioMedInformatics*, *2*(4), 603–624. https://doi.org/10.3390/biomedinformatics2040039

Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2). https://doi.org/10.1177/2053951716679679

Morse, S., Mazet, J., Woolhouse, M., Parrish, C., Carroll, D., Karesh, W., Zambrana-Torrelio, C., Lipkin, W., & Daszak, P. (2012). Prediction and prevention of the next pandemic zoonosis. *Lancet*, *380*(9857), 1956–1965. https://doi.org/10.1016/S0140-6736(12)61684-5

Mumuni, A., & Mumuni, F. (2022). Data augmentation: A comprehensive survey of modern approaches. *Array*, *16*, 100258. https://doi.org/10.1016/j.array.2022.10025

Navigli, R., Conia, S., & Ross, B. (2023). Biases in Large Language Models: Origins, Inventory, and Discussion. *Journal of Data and Information Quality*, *15*(2), 10. https://doi.org/10.1145/3597307

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

O'Reilly-Shah, V., Gentry, K., van Cleve, W., Kendale, S., Jabaley, C., & Long, D. (2020). The COVID-19 pandemic highlights shortcomings in US health care informatics infrastructure: a call to action. *Anesthesia & Analgesia*, *131*(2), 340–344. https://doi.org/10.1213/ANE.0000000000004945

Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, *39*(2), 230–253. https://doi.org/10.1518/001872097778543886

Parasuraman, R., Sheridan, T., & Wickens, C. (2000). A model for types and levels of human interaction with automation. *Systems and Humans*, *30*(3), 286–297. https://doi.org/10.1109/3468.844354

Pedro, R. (2022). Traços gerais da indemnização civil extracontratual pública em contextos de excecionalidade. In *Impactos da pandemia da Covid-19 nas estruturas do direito público* (pp. 379–413). Coimbra: Almedina. (In Portuguese).

Pedro, R. (2023). Inteligência artificial e arbitragem de direito público: Primeiras reflexões. In R. Pedro, & P. Caliendo (Coords.), *Inteligência artificial no contexto do direito público: Portugal e Brasil* (1.ª ed., pp. 105–127). Coimbra: Almedina. (In Portuguese).

Romano, A., Spadaro, G., Balliet, D., Joireman, J., van Lissa, C., Jin, S., ... & Leander, N. P. (2021). Cooperation and trust across societies during the COVID-19 pandemic. *Journal of Cross-Cultural Psychology*, *52*(7), 622–642. https://doi.org/10.1177/00220221209889

Ruan, W., Yi, X., & Huang, X. (2021). Adversarial robustness of deep learning: Theory, algorithms, and applications. In *Proceedings of the 30th ACM International Conference on Information & Knowledge Management* (pp. 4866–4869). https://doi.org/10.48550/arXiv.2108.10451

Rubin, O., Errett, N., Upshur, R., & Baekkeskov, E. (2021). The challenges facing evidence-based decision making in the initial response to COVID-19. *Scandinavian Journal of Public Health*, *49*(7), 790–796. https://doi.org/10.1177/140349482199722

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Sass, J., Bartschke, A., Lehne, M., Essenwanger, A., Rinaldi, E., Rudolph, S., ... & Thun, S. (2020). The German Corona Consensus Dataset (GECCO): a standardized dataset for COVID-19 research in university medicine and beyond. *BMC Medical Informatics and Decision Making*, *20*, 341. https://doi.org/10.1186/s12911-020-01374-w

Shin, D., & Park, Y. (2019). Role of fairness, accountability, and transparency in algorithmic affordance. *Computers in Human Behavior*, *98*, 277–284. https://doi.org/10.1016/j.chb.2019.04.019

Shaelou, S. L., & Razmetaeva, Y. (2023). Challenges to fundamental human rights in the age of artificial intelligence systems: Shaping the digital legal order while upholding rule of law principles and European values. *ERA Forum*, *24*(3), 567–587. https://doi.org/10.1007/s12027-023-00777-2

Silva, M., Flood, C., Goldenberg, A., & Singh, D. (2022). Regulating the Safety of Health-Related Artificial Intelligence. *Healthcare Policy*, *17*(4), 63–77. https://doi.org/10.12927/hcpol.2022.26824

Smidt, H., & Jokonya, O. (2021). The challenge of privacy and security when using technology to track people in times of COVID-19 pandemic. *Procedia Computer Science*, *181*, 1018–1026. https://doi.org/10.1016/j.procs.2021.01.281

Sundar, S. (2020). Rise of machine agency: A framework for studying the psychology of human – AI interaction (HAII). *Journal of Computer-Mediated Communication*, *25*(1), 74–88. https://doi.org/10.1093/jcmc/zmz026

Susskind, D. (2021). A world without work: Technology, automation and how we should respond. New Technology, *Work and Employment*, *36*(1), 114-117. https://doi.org/10.1111/ntwe.12186

Syed, R., Ulbricht, M., Piotrowski, K., & Krstic, M. (2023). A Survey on Fault-Tolerant Methodologies for Deep Neural Networks. *Pomiary Automatyka Robotyka*, *27*(2), 89–98. https://doi.org/10.14313/PAR_248/89

Syrowatka, A., Kuznetsova, M., Alsubai, A., Beckman, A., Bain, P., Craig, K., ... & Bates, D. (2021). Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases. *npj Digital Medicine*, *4*(1), 96. https://doi.org/10.1038/s41746-021-00459-8

Theis, T., & Wong, H. (2017). The end of Moore's law: A new beginning for information technology. *Computing in Science & Engineering*, *19*(2), 41–50. https://doi.org/10.1109/MCSE.2017.29

Thomsen, K. (2019). Ethics for artificial intelligence, ethics for all. *Paladyn, Journal of Behavioral Robotics*, *10*(1), 359–363. https://doi.org/10.1515/pjbr-2019-0029

Topol, E. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Villegas-Ch, W., Jaramillo-Alcázar, A., & Luján-Mora, S. (2024). Evaluating the Robustness of Deep Learning Models against Adversarial Attacks: An Analysis with FGSM, PGD and CW. *Big Data and Cognitive Computing*, *8*(1), 8. https://doi.org/10.3390/bdcc8010008

Vopson, M. (2020). The information catastrophe. *AIP Advances*, *10*(8), 085014. https://doi.org/10.1063/5.0019941

Wallach W., & Allen, C. (2008). *Moral Machines: Teaching Robots Right from Wrong*. Oxford University Press.

Wang, S., & Shi, W. (2011). Data Mining and Knowledge Discovery. In W. Kresse, D. Danko (Eds.), *Springer Handbook of Geographic Information*. Springer Handbooks. https://doi.org/10.1007/978-3-540-72680-7_5

Wong, F., de la Fuente-Nunez, C., & Collins, J. (2023). Leveraging artificial intelligence in the fight against infectious diseases. *Science*, *381*(6654), 164–170. https://doi.org/10.1126/science.adh1114

Wu, D., Xu, H., Yongyi, W., & Zhu, H. (2022). Quality of government health data in COVID-19: definition and testing of an open government health data quality evaluation framework. *Library Hi Tech*, *40*(2), 516–534. https://doi.org/10.1108/LHT-04-2021-0126

Zhang, Q., Gao, J., Wu, J., Cao, Z., & Dajun, D. (2022). Data science approaches to confronting the COVID-19 pandemic: a narrative review. *Philosophical Transactions of the Royal Society A*, *380*(2214), 20210127. https://doi.org/10.1098/rsta.2021.0127

Zhou, J., Zheng, W., Wang, D., & Coit, D. W. (2024). A resilient network recovery framework against cascading failures with deep graph learning. *Journal of Risk and Reliability*, *238*(1), 193–203. https://doi.org/10.1177/1748006X22112886

Сведения об авторах

Коррейя Педро Мигель Алвес Рибейро – PhD в области общественных наук (государственное управление), приглашенный доцент, юридический факультет, Коимбрский университет; приглашенный профессор, ICET/CUA/UFMT, Барра до Гарсас
Адрес: Португалия, 3004-528, г. Коимбра, Патио да Универсидаде; Бразилия, 78605-091, Авенида Валдон Варжан, 6390, Барра до Гарсас – MT, CEP
E-mail: pcorreia@fd.uc.pt
ORCID ID: https://orcid.org/0000-0002-3111-9843
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58223408400
WoS Researcher ID: https://www.webofscience.com/wos/author/record/B-2753-2015
Google Scholar ID: https://scholar.google.pt/citations?user=KABKPuUAAAAJ

Рикардо Лопес Динис Педро – PhD в области права, научный сотрудник, Лиссабонский исследовательский центр в области публичного права, юридический факультет, Лиссабонский университет
Адрес: Португалия, 1649-014, г. Лиссабон, Аламеда де Универсидаде
E-mail: ricardopedro@fd.ulisboa.pt
ORCID ID: https://orcid.org/0000-0001-6339-5140
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57879177700
WoS Researcher ID: https://www.webofscience.com/wos/author/record/AEN-4511-2022
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=oJ1ImgUAAAAJ

Сусана Видейра – PhD в области права, доцент, юридический факультет, Лиссабонский университет; координатор по науке и образованию, Европейский университет в Лиссабоне
Адрес: Португалия, 1649-014, г. Лиссабон, Аламеда де Универсидаде; Португалия, 1500-210, г. Лиссабон, Эстрада да Коррейя, 53
E-mail: susanavideira@fd.ulisboa.pt
ORCID ID: https://orcid.org/0000-0002-9246-2557

Вклад авторов

Авторы внесли равный вклад в разработку концепции, методологии, валидацию, формальный анализ, проведение исследования, подбор источников, написание и редактирование текста, руководство и управление проектом.

Конфликт интересов

Авторы сообщают об отсутствии конфликта интересов.

Финансирование

Участие автора Рикардо Лопес Динис Педро частично финансировалось Фондом науки и технологий Португалии (Foundation for Science and Technology, FCT) в рамках проекта UIDP/04310/2020. Исследование также было поддержано тем же Фондом в рамках проекта UIDB/04643/2020.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.15.59 / Права и свободы человека и гражданина
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 15 июня 2024 г.
Дата одобрения после рецензирования – 27 июня 2024 г.
Дата принятия к опубликованию – 25 марта 2025 г.
Дата онлайн-размещения – 30 марта 2025 г.

Research article
UDC 34:004:17:004.8:342.7
EDN: https://elibrary.ru/egkppn
DOI: https://doi.org/10.21202/jdtl.2025.7

Artificial Intelligence in Healthcare: Balancing Innovation, Ethics, and Human Rights Protection

Pedro Miguel Alves Ribeiro Correia ✉
University of Coimbra, Coimbra, Portugal

Ricardo Lopes Dinis Pedro
Lisbon Public Law Research Centre University of Lisbon

Susana Videira
University of Lisbon, Lisboa, Portugal

Keywords

artificial intelligence,
data protection,
ethical regulation,
ethics,
fundamental rights,
healthcare,
human rights,
law,
legal regulation,
predictive analytics

Abstract

Objective: to identify key ethical, legal and social challenges related to the use of artificial intelligence in healthcare; to develop recommendations for creating adaptive legal mechanisms that can ensure a balance between innovation, ethical regulation and the protection of fundamental human rights.

Methods: a multidimensional methodological approach was implemented, integrating classical legal analysis methods with modern tools of comparative jurisprudence. The study covers both the fundamental legal regulation of digital technologies in the medical field and the in-depth analysis of the ethical, legal and social implications of using artificial intelligence in healthcare. Such an integrated approach provides a comprehensive understanding of the issues and well-grounded conclusions about the development prospects in this area.

Results: has revealed a number of serious problems related to the use of artificial intelligence in healthcare. These include data bias, non-transparent complex algorithms, and privacy violation risks. These problems can undermine public confidence in artificial intelligence technologies and exacerbate inequalities in access to health services. The authors conclude that the integration of artificial intelligence into healthcare should take into account fundamental rights, such as data protection and non-discrimination, and comply with ethical standards.

✉ Corresponding author

Scientific novelty: the work proposes effective mechanisms to reduce risks and maximize the potential of artificial intelligence under crises. Special attention is paid to regulatory measures, such as the impact assessment provided for by the Artificial Intelligence Act. These measures play a key role in identifying and minimizing the risks associated with high-risk artificial intelligence systems, ensuring compliance with ethical standards and protection of fundamental rights.

Practical significance: adaptive legal mechanisms were developed, that support democratic norms and respond promptly to emerging challenges in public healthcare. The proposed mechanisms allow achieving a balance between using artificial intelligence for crisis management and human rights. This helps to build confidence in artificial intelligence systems and their sustained positive impact on public healthcare.

For citation

Correia, P. M. A. R., Pedro, R. L. D., & Videira, S. (2025). Artificial Intelligence in Healthcare: Balancing Innovation, Ethics, and Human Rights Protection. *Journal of Digital Technologies and Law, 3*(1), 143–180. https://doi.org/10.21202/jdtl.2025.7

References

Arass, M., & Souissi, N. (2018). Data lifecycle: from big data to SmartData. In *2018 IEEE 5th International Congress on Information Science and Technology* (pp. 80–87). IEEE. https://doi.org/10.1109/CIST.2018.8596547

Alvarez Garcia, V. (1996). *El concepto de necesidad en derecho público* (1st ed.). Madrid: Civitas. (In Spanish).

Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., ... & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion*, *58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012

Baclic, O., Tunis, M., Young, K., Doan, C., Swerdfeger, H., & Schonfeld, J. (2020). Challenges and opportunities for public health made possible by advances in natural language processing. *Canada Communicable Disease Report*, *46*(6), 161–168. https://doi.org/10.14745/ccdr.v46i06a02

Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: transforming the practice of medicine. *Future Healthcare Journal*, *8*(2), e188-e194. https://doi.org/10.7861/fhj.2021-0095

Beck, U. (1986). *Risikogesellschaft: Auf dem Weg in eine andere Moderne*. Frankfurt am Main: Suhrkamp Verlag.

Balog-Way, D., & McComas, K. (2022). COVID-19: Reflections on trust, tradeoffs, and preparedness. In *COVID-19* (pp. 6–16). Routledge.

Bazarkina, D. Y., & Pashentsev, E. N. (2020). Malicious use of artificial intelligence. *Russia in Global Affairs*, *18*(4), 154–177. https://doi.org/10.31278/1810-6374-2020-18-4-154-177

Benke, K., & Benke, G. (2018). Artificial Intelligence and Big Data in Public Health. *International Journal of Environmental Research and Public Health*, *15*(12), 2796. https://doi.org/10.3390/ijerph15122796

Berk, R. A. (1983). An introduction to sample selection bias in sociological data. *American Sociological Review*, *48*(3), 386–398. https://doi.org/10.2307/2095230

Bigham, G., Adamtey, S., Onsarigo, L., & Jha, N. (2019). Artificial Intelligence for Construction Safety: Mitigation of the Risk of Fall. In K. Arai, S. Kapoor, R. Bhatia (Eds.). *Intelligent Systems and Applications*. Springer. https://doi.org/10.1007/978-3-030-01057-7_76

Binder, W. (2024). Technology as (dis-)enchantment. AlphaGo and the meaning-making of artificial intelligence. *Cultural Sociology*, *18*(1), 24–47. https://doi.org/10.1177/17499755221138720

Bisconti, P., Orsitto, D., Fedorczyk, F., Brau, F., Capasso, M., De Marinis, L., ... & Schettini, C. (2023). Maximizing team synergy in AI-related interdisciplinary groups: an interdisciplinary-by-design iterative methodology. *AI & Society*, *38*(4), 1443–1452. https://doi.org/10.1007/s00146-022-01518-8

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

Box, G. (1979). Robustness in the strategy of scientific model building. In R. Launer & G. Wilkinson (Eds.), *Robustness in Statistics* (pp. 201–236). Academic Press. https://doi.org/10.1016/B978-0-12-438150-6.50018-2

Breiman, L. (2001). Statistical Modeling: The Two Cultures (with comments and a rejoinder by the author). *Statistical Science*, *16*(3), 199–231. https://doi.org/10.1214/ss/1009213726

Bulled, N. (2023). "Solidarity:" A failed call to action during the COVID-19 pandemic. *Public Health in Practice*, *5*, 100379. https://doi.org/10.1016/j.puhip.2023.100379

Chen, A. (2016). A review of emerging non-volatile memory (NVM) technologies and applications. *Solid-State Electronics*, *125*, 25–38. https://doi.org/10.1016/j.sse.2016.07.006

Chen, J., Zhang, R., Han, W., Jiang, W., Hu, J., Lu, X., Liu, X., & Zhao, P. (2020). Path Planning for Autonomous Vehicle Based on a Two-Layered Planning Model in Complex Environment. *Journal of Advanced Transportation*, 2020, 6649867. https://doi.org/10.1155/2020/6649867

Chiao, V. (2019). Fairness, accountability and transparency: notes on algorithmic decision-making in criminal justice. *International Journal of Law in Context*, *15*(2), 126–139. https://doi.org/10.1017/S1744552319000077

Correia, P., Mendes, I., Pereira, S., & Subtil, I. (2020a). The combat against COVID-19 in Portugal: How state measures and data availability reinforce some organizational values and contribute to the sustainability of the National Health System. *Sustainability*, *12*(18), 7513. https://doi.org/10.3390/su12187513

Correia, P., Mendes, I., Pereira, S., & Subtil, I. (2020b). The combat against COVID-19 in Portugal, Part II: how governance reinforces some organizational values and contributes to the sustainability of crisis management. *Sustainability*, *12*(20), 8715. https://doi.org/10.3390/su12208715

Correia, P., Pereira, S., Mendes, I., & Subtil, I. (2022). COVID-19 Crisis management and the Portuguese regional governance: Citizens perceptions as evidence. *European Journal of Applied Business Management*, *8*(1), 1–12.

Correia, P., Pereira, S., Mendes, I., & Subtil, I. (2021). COVID-19 Crisis management and the Portuguese regional governance: Citizens perceptions as evidence. In *European Consortium for Political Research General Conference* (pp. 1–18). United Kingdom.

Correia, J. M. C. (1987). *Legalidade e autonomia contratual nos contratos administrativos* (pp. 283, 768). Lisboa: Almedina.

DeCamp, M., & Tilburt, J. (2019). Why we cannot trust artificial intelligence in medicine. *The Lancet Digital health*, *1*(8), e390. https://doi.org/10.1016/S2589-7500(19)30197-9

Dhingra, M., & Gupta, N. (2017). Comparative analysis of fault tolerance models and their challenges in cloud computing. *International Journal of Engineering & Technology*, *6*(2), 36–40. https://doi.org/10.14419/ijet.v6i2.7565

Ettlinger, N. (2022). *Algorithms and the Assault on Critical Thought: Digitalized Dilemmas of Automated Governance and Communitarian Practice* (1st ed.). Routledge. https://doi.org/10.4324/9781003109792

Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. New York: Picador, St Martin's Press.

Ferguson, N., Cummings, D., Fraser, C., Cajka, J., Cooley, P., & Burke, D. (2006). Strategies for mitigating an influenza pandemic. *Nature*, *442*(7101), 448–452. https://doi.org/10.1038/nature04795

Fetzer, T., & Graeber, T. (2021). Measuring the scientific effectiveness of contact tracing: Evidence from a natural experiment. *Proceedings of the National Academy of Sciences of the United States of America*, *118*(33), e2100814118. https://doi.org/10.1073/pnas.2100814118

Galetsi, P., Katsaliaki, K., & Kumar, S. (2022). The medical and societal impact of big data analytics and artificial intelligence applications in combating pandemics: A review focused on Covid-19. *Social Science & Medicine*, *301*, 114973. https://doi.org/10.1016/j.socscimed.2022.114973

Gianfrancesco, M., Tamang, S., Yazdany, J., & Schmajuk, G. (2018). Potential Biases in Machine Learning Algorithms Using Electronic Health Record Data. *JAMA Internal Medicine*, *178*(11), 1544–1547. https://doi.org/10.1001/jamainternmed.2018.3763

Goldman, N., Bertone, P., Chen, S., Dessimoz, C., LeProust, E. M., Sipos, B., & Birney, E. (2013). Towards practical, high-capacity, low-maintenance information storage in synthesized DNA. *Nature*, *494*(7435), 77–80. https://doi.org/10.1038/nature11875

Gomes, C. A., & Pedro, R. (Coords.). (2020). *Direito administrativo de necessidade e de excepção*. Lisboa: AAFDL.

Gómez Abeja, L. (2022). Inteligencia artificial y derechos fundamentales. In F. H. Llano Alonso (Dir.), J. Garrido Martín & R. Valdivia Jiménez (Coords.), *Inteligencia artificial y filosofía del derecho* (1.ª ed., pp. 91–114, 93). Murcia: Ediciones Laborum. (In Spanish).

Gómez Colomer, J.-L. (2023). *El juez-robot: La independencia judicial en peligro*. Valencia: Tirant lo Blanch. (In Spanish).

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press.
Greiner, R., Grove, A., & Kogan, A. (1997). Knowing what doesn't matter: exploiting the omission of irrelevant data. *Artificial Intelligence*, *97*(1–2), 345–380. https://doi.org/10.1016/S0004-3702(97)00048-9
Gunasekeran, D., Tseng, R., Tham, Y., & Wong, T. (2021). Applications of digital health for public health responses to COVID-19: a systematic scoping review of artificial intelligence, telehealth and related technologies. *NPJ Digital Medicine*, *4*(1), 40. https://doi.org/10.1038/s41746-021-00412-9
Gürsoy, E., & Kaya, Y. (2023). An overview of deep learning techniques for COVID-19 detection: methods, challenges, and future works. *Multimedia Systems*, *29*(3), 1603–1627. https://doi.org/10.1007/s00530-023-01083-0
Hanegraaff, W. (2013). *Western Esotericism: A Guide for the Perplexed*. Bloomsbury Publishing.
Halevy, A., Norvig, P., & Pereira, F. (2009). The unreasonable effectiveness of data. *IEEE Intelligent Systems*, 24(2), 8–12. https://doi.org/10.1109/MIS.2009.36
Hazarika, I. (2020). Artificial intelligence: opportunities and implications for the health workforce. *International Health*, *12*(4), 241–245. https://doi.org/10.1093/inthealth/ihaa007
Hoff, K., & Bashir, M. (2015). Trust in automation: Integrating empirical evidence on factors that influence trust. *Human Factors*, *57*(3), 407–434. https://doi.org/10.1177/0018720814547570
Hulten, G. (2018). Building Intelligent Systems: A Guide to Machine Learning Engineering. Apress.
Igual, L., & Seguí, S. (2024). *Supervised learning. In Introduction to Data Science: A Python Approach to Concepts, Techniques and Applications* (pp. 67–97). Springer International Publishing.
Jiang, F., Jiang, Y., Zhi, H., Dong, Y., Li, H., Ma, S., Wang, Y., Dong, Q., Shen, H., & Wang, Y. (2017). Artificial intelligence in healthcare: past, present and future. *Stroke and Vascular Neurology*, *2*(4), 230–243. https://doi.org/10.1136/svn-2017-000101
Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*, 389–399. https://doi.org/10.1038/s42256-019-0088-2
Jones, K., Patel, N., Levy, M., Storeygard, A., Balk, D., Gittleman, J., & Daszak, P. (2008). Global trends in emerging infectious diseases. *Nature*, *451*(7181), 990–993. https://doi.org/10.1038/nature06536
Kandlhofer, M., Weixelbraun, P., Menzinger, M., Steinbauer-Wagner, G., & Kemenesi, Á. (2023). Education and Awareness for Artificial Intelligence. In *International Conference on Informatics in Schools: Situation, Evolution, and Perspectives* (pp. 3–12). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-44900-0_1
Kavanagh, J., & Rich, M. (2018). *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life*. RAND Corporation. https://doi.org/10.7249/RR2314
Kirkpatrick, J., Pascanu, R., Rabinowitz, N., Veness, J., Desjardins, G., Rusu, A. A., ... & Hadsell, R. (2017). Overcoming catastrophic forgetting in neural networks. *Proceedings of the National Academy of Sciences*, *114*(13), 3521–3526. https://doi.org/10.1073/pnas.1611835114
Kordzadeh, N., & Ghasemaghaei, M. (2022). Algorithmic bias: review, synthesis, and future research directions. E*uropean Journal of Information Systems*, *31*(3), 388–409. https://doi.org/10.1080/0960085X.2021.1927212
Larsson, S., & Heintz, F. (2020). Transparency in artificial intelligence. *Internet Policy Review*, *9*(2). https://doi.org/10.14763/2020.2.1469
Lin, X., Liu, J., Hao, J., Wang, K., Zhang, Y., Li, H., ... & Tan, X. (2020). Collinear holographic data storage technologies. *Opto-Electronic Advances*, *3*(3), 190004. https://doi.org/10.29026/oea.2020.190004
Little, R. J., & Rubin, D. B. (2019). Statistical analysis with missing data. John Wiley & Sons.
Macrae, C. (2022). Learning from the failure of autonomous and intelligent systems: Accidents, safety, and sociotechnical sources of risk. *Risk Analysis*, *42*(9), 1999–2025. https://doi.org/10.1111/risa.13850
Margetts, H. (2022). Rethinking AI for good governance. *Daedalus*, *151*(2), 360–371. https://doi.org/10.1162/daed_a_01922
Matsuzaka, Y., & Yashiro, R. (2022). Applications of Deep Learning for Drug Discovery Systems with BigData. *BioMedInformatics*, *2*(4), 603–624. https://doi.org/10.3390/biomedinformatics2040039
Mittelstadt, B., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, *3*(2). https://doi.org/10.1177/2053951716679679
Morse, S., Mazet, J., Woolhouse, M., Parrish, C., Carroll, D., Karesh, W., Zambrana-Torrelio, C., Lipkin, W., & Daszak, P. (2012). Prediction and prevention of the next pandemic zoonosis. *Lancet*, *380*(9857), 1956–1965. https://doi.org/10.1016/S0140-6736(12)61684-5
Mumuni, A., & Mumuni, F. (2022). Data augmentation: A comprehensive survey of modern approaches. *Array*, *16*, 100258. https://doi.org/10.1016/j.array.2022.10025
Navigli, R., Conia, S., & Ross, B. (2023). Biases in Large Language Models: Origins, Inventory, and Discussion. *Journal of Data and Information Quality*, *15*(2), 10. https://doi.org/10.1145/3597307

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447–453. https://doi.org/10.1126/science.aax2342

O'Reilly-Shah, V., Gentry, K., van Cleve, W., Kendale, S., Jabaley, C., & Long, D. (2020). The COVID-19 pandemic highlights shortcomings in US health care informatics infrastructure: a call to action. *Anesthesia & Analgesia*, *131*(2), 340–344. https://doi.org/10.1213/ANE.0000000000004945

Parasuraman, R., & Riley, V. (1997). Humans and Automation: Use, Misuse, Disuse, Abuse. *Human Factors*, *39*(2), 230–253. https://doi.org/10.1518/001872097778543886

Parasuraman, R., Sheridan, T., & Wickens, C. (2000). A model for types and levels of human interaction with automation. *Systems and Humans*, *30*(3), 286–297. https://doi.org/10.1109/3468.844354

Pedro, R. (2022). Traços gerais da indemnização civil extracontratual pública em contextos de excecionalidade. In *Impactos da pandemia da Covid-19 nas estruturas do direito público* (pp. 379–413). Coimbra: Almedina. (In Portuguese).

Pedro, R. (2023). Inteligência artificial e arbitragem de direito público: Primeiras reflexões. In R. Pedro, & P. Caliendo (Coords.), *Inteligência artificial no contexto do direito público: Portugal e Brasil* (1.ª ed., pp. 105–127). Coimbra: Almedina. (In Portuguese).

Romano, A., Spadaro, G., Balliet, D., Joireman, J., van Lissa, C., Jin, S., ... & Leander, N. P. (2021). Cooperation and trust across societies during the COVID-19 pandemic. *Journal of Cross-Cultural Psychology*, *52*(7), 622–642. https://doi.org/10.1177/00220221209889

Ruan, W., Yi, X., & Huang, X. (2021). Adversarial robustness of deep learning: Theory, algorithms, and applications. In *Proceedings of the 30th ACM International Conference on Information & Knowledge Management* (pp. 4866–4869). https://doi.org/10.48550/arXiv.2108.10451

Rubin, O., Errett, N., Upshur, R., & Baekkeskov, E. (2021). The challenges facing evidence-based decision making in the initial response to COVID-19. *Scandinavian Journal of Public Health*, *49*(7), 790–796. https://doi.org/10.1177/140349482199722

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach* (4th ed.). Pearson.

Sass, J., Bartschke, A., Lehne, M., Essenwanger, A., Rinaldi, E., Rudolph, S., ... & Thun, S. (2020). The German Corona Consensus Dataset (GECCO): a standardized dataset for COVID-19 research in university medicine and beyond. *BMC Medical Informatics and Decision Making*, *20*, 341. https://doi.org/10.1186/s12911-020-01374-w

Shin, D., & Park, Y. (2019). Role of fairness, accountability, and transparency in algorithmic affordance. *Computers in Human Behavior*, *98*, 277–284. https://doi.org/10.1016/j.chb.2019.04.019

Shaelou, S. L., & Razmetaeva, Y. (2023). Challenges to fundamental human rights in the age of artificial intelligence systems: Shaping the digital legal order while upholding rule of law principles and European values. *ERA Forum*, *24*(3), 567–587. https://doi.org/10.1007/s12027-023-00777-2

Silva, M., Flood, C., Goldenberg, A., & Singh, D. (2022). Regulating the Safety of Health-Related Artificial Intelligence. *Healthcare Policy*, *17*(4), 63–77. https://doi.org/10.12927/hcpol.2022.26824

Smidt, H., & Jokonya, O. (2021). The challenge of privacy and security when using technology to track people in times of COVID-19 pandemic. *Procedia Computer Science*, *181*, 1018–1026. https://doi.org/10.1016/j.procs.2021.01.281

Sundar, S. (2020). Rise of machine agency: A framework for studying the psychology of human – AI interaction (HAII). *Journal of Computer-Mediated Communication*, *25*(1), 74–88. https://doi.org/10.1093/jcmc/zmz026

Susskind, D. (2021). A world without work: Technology, automation and how we should respond. New Technology, *Work and Employment*, *36*(1), 114-117. https://doi.org/10.1111/ntwe.12186

Syed, R., Ulbricht, M., Piotrowski, K., & Krstic, M. (2023). A Survey on Fault-Tolerant Methodologies for Deep Neural Networks. *Pomiary Automatyka Robotyka*, *27*(2), 89–98. https://doi.org/10.14313/PAR_248/89

Syrowatka, A., Kuznetsova, M., Alsubai, A., Beckman, A., Bain, P., Craig, K., ... & Bates, D. (2021). Leveraging artificial intelligence for pandemic preparedness and response: a scoping review to identify key use cases. *npj Digital Medicine*, *4*(1), 96. https://doi.org/10.1038/s41746-021-00459-8

Theis, T., & Wong, H. (2017). The end of Moore's law: A new beginning for information technology. *Computing in Science & Engineering*, *19*(2), 41–50. https://doi.org/10.1109/MCSE.2017.29

Thomsen, K. (2019). Ethics for artificial intelligence, ethics for all. *Paladyn, Journal of Behavioral Robotics*, *10*(1), 359–363. https://doi.org/10.1515/pjbr-2019-0029

Topol, E. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56. https://doi.org/10.1038/s41591-018-0300-7

Villegas-Ch, W., Jaramillo-Alcázar, A., & Luján-Mora, S. (2024). Evaluating the Robustness of Deep Learning Models against Adversarial Attacks: An Analysis with FGSM, PGD and CW. *Big Data and Cognitive Computing*, *8*(1), 8. https://doi.org/10.3390/bdcc8010008

Vopson, M. (2020). The information catastrophe. *AIP Advances*, *10*(8), 085014. https://doi.org/10.1063/5.0019941

Wallach W., & Allen, C. (2008). *Moral Machines: Teaching Robots Right from Wrong*. Oxford University Press.

Wang, S., & Shi, W. (2011). Data Mining and Knowledge Discovery. In W. Kresse, D. Danko (Eds.), *Springer Handbook of Geographic Information*. Springer Handbooks. https://doi.org/10.1007/978-3-540-72680-7_5

Wong, F., de la Fuente-Nunez, C., & Collins, J. (2023). Leveraging artificial intelligence in the fight against infectious diseases. *Science*, *381*(6654), 164–170. https://doi.org/10.1126/science.adh1114

Wu, D., Xu, H., Yongyi, W., & Zhu, H. (2022). Quality of government health data in COVID-19: definition and testing of an open government health data quality evaluation framework. *Library Hi Tech*, *40*(2), 516–534. https://doi.org/10.1108/LHT-04-2021-0126

Zhang, Q., Gao, J., Wu, J., Cao, Z., & Dajun, D. (2022). Data science approaches to confronting the COVID-19 pandemic: a narrative review. *Philosophical Transactions of the Royal Society A*, *380*(2214), 20210127. https://doi.org/10.1098/rsta.2021.0127

Zhou, J., Zheng, W., Wang, D., & Coit, D. W. (2024). A resilient network recovery framework against cascading failures with deep graph learning. *Journal of Risk and Reliability*, *238*(1), 193–203. https://doi.org/10.1177/1748006X22112886

Authors information

Pedro Miguel Alves Ribeiro Correia – PhD in Social Sciences (Specialty in Public Administration), Invited Associate Professor, Faculty of Law, University of Coimbra; Visiting Full Professor, ICET/CUA/UFMT, Barra do Garças
Address: Pátio da Universidade, 3004-528 Coimbra, Portugal;
Avenida ValdonVarjão, n. 6390, Barra do Garças – MT, CEP: 78605-091, Brazil
E-mail: pcorreia@fd.uc.pt
ORCID ID: https://orcid.org/0000-0002-3111-9843
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=58223408400
WoS Researcher ID: https://www.webofscience.com/wos/author/record/B-2753-2015
Google Scholar ID: https://scholar.google.pt/citations?user=KABKPuUAAAAJ

Ricardo Lopes Dinis Pedro – PhD (Law), Researcher, Lisbon Public Law Research Centre, Faculty of Law, University of Lisbon
Address: Alameda da Universidade, 1649-014 Lisbon, Portugal
E-mail: ricardopedro@fd.ulisboa.pt
ORCID ID: https://orcid.org/0000-0001-6339-5140
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57879177700
WoS Researcher ID: https://www.webofscience.com/wos/author/record/AEN-4511-2022
Google Scholar ID: https://scholar.google.com/citations?hl=en&user=oJ1ImgUAAAAJ

Susana Videira – PhD (Law), Associate Professor, Faculty of Law, University of Lisbon; Scientific and Pedagogical Coordinator, Law Degree and the Master's Degree in Judicial Law, European University
Address: Faculdade de Direito da Universidade de Lisboa, Alameda da Universidade, 1649-014 Lisbon, Portugal; Universidade Europeia, Estrada da Correia, n.º 53, 1500-210, Lisbon, Portugal
E-mail: susanavideira@fd.ulisboa.pt
ORCID ID: https://orcid.org/0000-0002-9246-2557

Authors' contributions

The authors have contributed equally into the concept and methodology elaboration, validation, formal analysis, research, selection of sources, text writing and editing, project guidance and management.

Conflict of interests

The authors declare no conflict of interests.

Financial disclosure

Regarding the participation of the Author Ricardo Pedro, it should be noted that, to the exact extent of his participation, the work is financed (or partially financed) by national funds through FCT–Foundation for Science and Technology, I.P., under the project UIDP/04310/2020. This work was also supported by Portuguese national funds through FCT–Foundation for Science and Technology, I.P., under project UIDB/04643/2020.

Thematic rubrics

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

Article history

Date of receipt – June 15, 2025
Date of approval – June 27, 2025
Date of acceptance – March 25, 2025
Date of online placement – March 30, 2025