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.

© Бхатт Н., 2025

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/deed.ru), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

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.

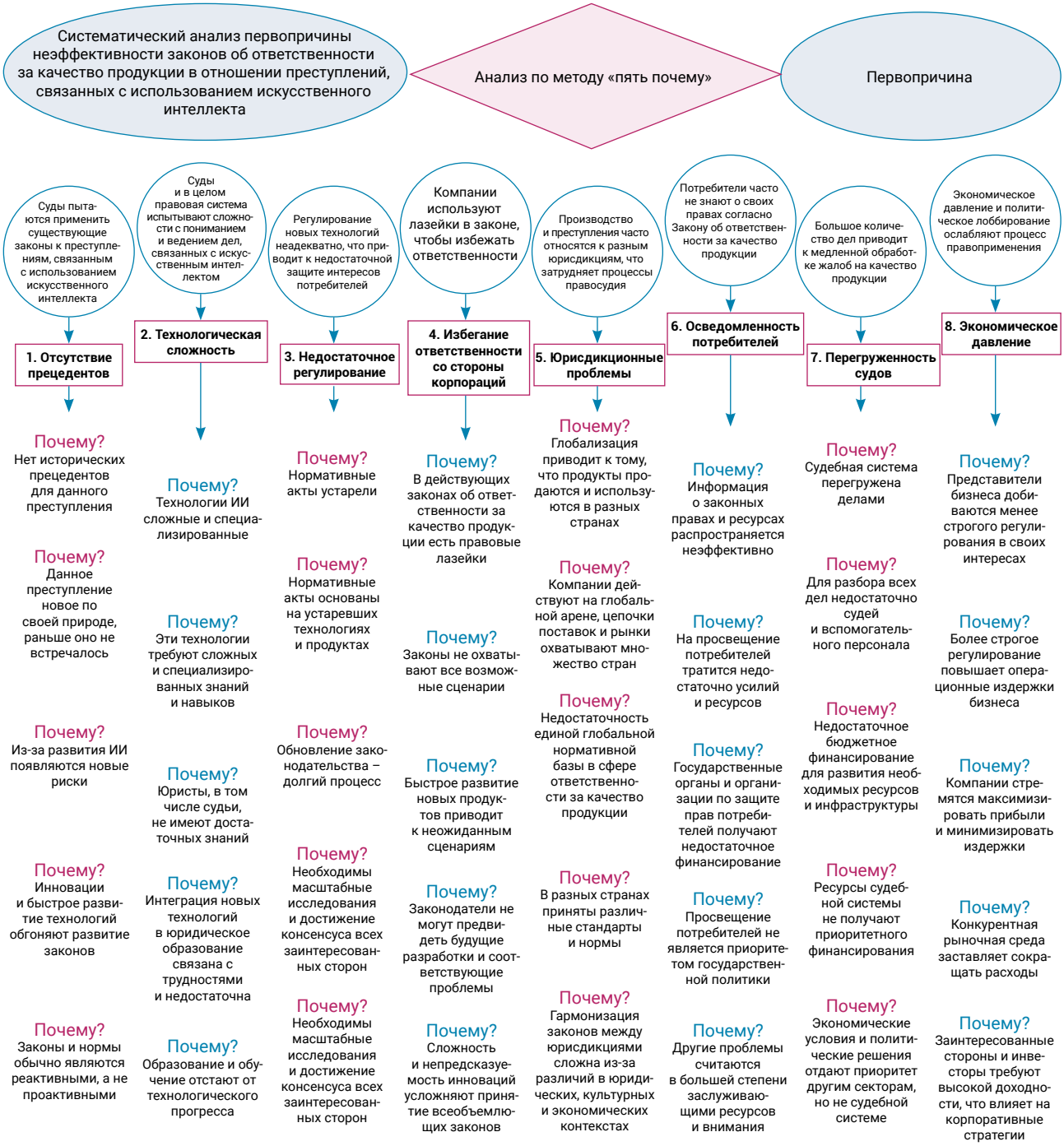

Рис. 3. Первопричины неэффективности законов об ответственности за качество продукции в отношении преступлений, связанных с использованием искусственного интеллекта

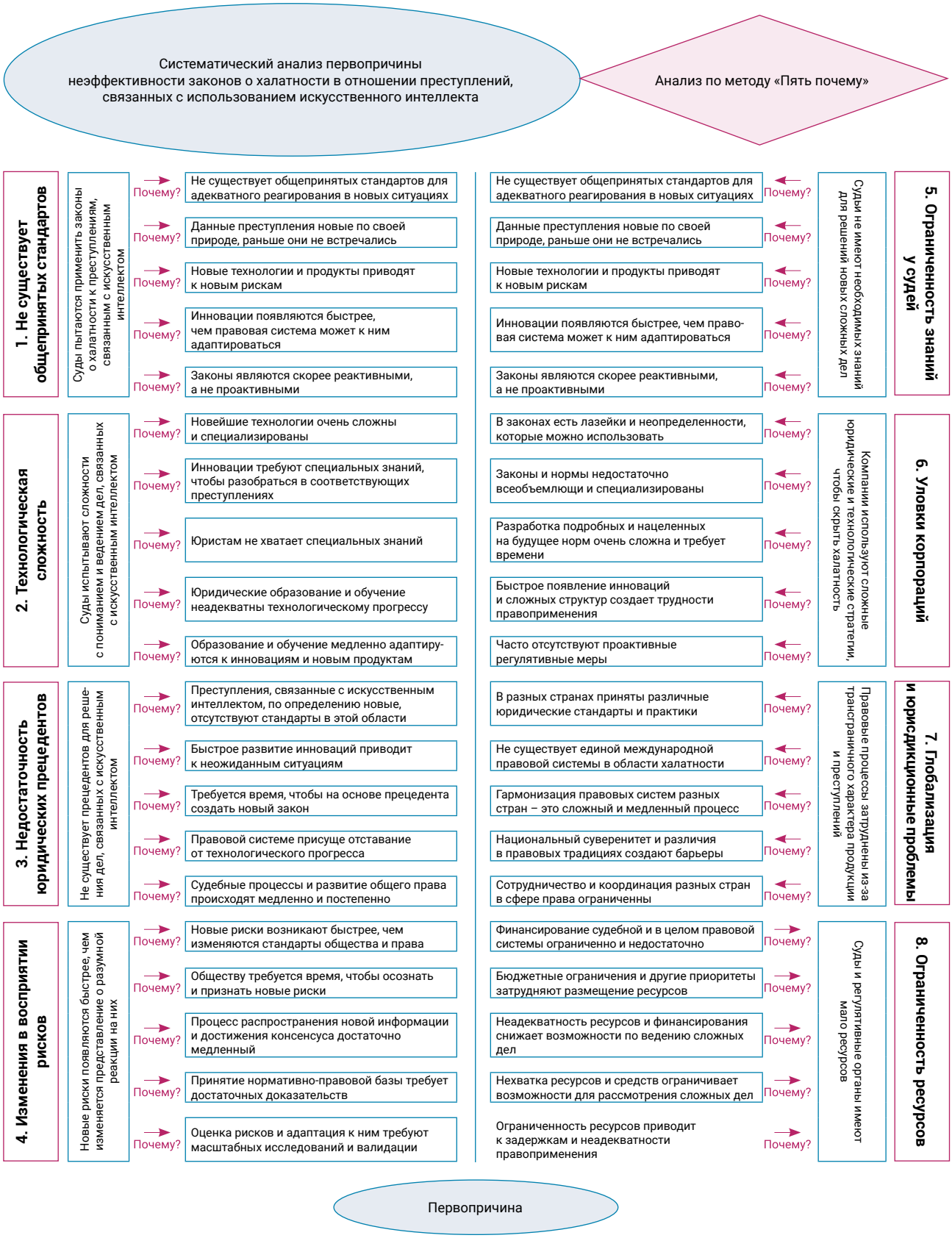

Рис. 4. Первопричины неэффективности законов о халатности в отношении преступлений, связанных с использованием искусственного интеллекта

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.

© Bhatt N., 2025

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

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