Публично-правовые (государственно-правовые) науки

Научная статья
УДК 342.9
doi: 10.35750/2071-8284-2023-3-67-75

Атабек Рустамович Атабеков
кандидат экономических наук
https://orcid.org/0000-0002-1456-7409, atabekov-ar@rudn.ru

Российский университет дружбы народов
Российская Федерация, 117198, Москва, ул. Миклухо-Маклая, д. 6

Вопросы осуществления предиктивного права в правоохранительной деятельности: сравнительно-правовое исследование

Аннотация: Статья представляет сравнительный анализ действующих подходов по применению искусственного интеллекта (ИИ) в сфере контрольно-надзорной деятельности со стороны правоохранительных органов зарубежных стран и России. Объектом исследования выступают нормативные акты, рекомендации и иные документы, регламентирующие вопросы применения искусственного интеллекта для осуществления правоохранительной деятельности, судебная практика, академические публикации и аналитические отчёты по исследуемой проблеме.

Методология исследования интегрирует комплекс современных философских, общенаучных, специально-научных методов познания, включая диалектический, системный, структурно-функциональный, герменевтический, сравнительно-правовой, формально-юридический (догматический) и др.

В рамках исследования делается акцент на осуществлении сравнительного правового исследования областей применения ИИ в правоохранительной деятельности и выработки единых подходов по регламентации применения ИИ и противодействия ИИ, применяемому в противоправной деятельности.

По результатам проведённого сравнительного анализа выявлены базовые проблемы в области обеспечения точности аналитических инструментов, используемых при расследовании преступлений и пресечении правонарушений, рассмотрены теоретические и практические ситуации применения искусственного интеллекта в правоохранительной деятельности, изучены отдельные примеры применения технологии deepfake в противоправной деятельности и механизмах противодействия указанной технологии.

В выводах предложены дополнительные компенсирующие правовые мероприятия, обеспечивающие эффективную интеграцию искусственного интеллекта и его использование для целей правоохранительных органов России.

Ключевые слова: искусственный интеллект, сравнительно-правовое исследование, предиктивное право, публичное право, правоприменительная практика

Для цитирования: Атабеков А. Р. Вопросы осуществления предиктивного права в правоохранительной деятельности: сравнительно-правовое исследование // Вестник Санкт-Петербургского университета МВД России. – 2023. – № 3 (99). – С. 67–75; doi: 10.35750/2071-8284-2023-3-67-75.

Atabek R. Atabekov
Cand. Sci. (Econ.)
https://orcid.org/0000-0002-1456-7409, atabekov-ar@rudn.ru

Peoples' Friendship University of Russia
6, Miklukho-Maklaya str., Moscow, 117198, Russian Federation

Issues in the implementation of predictive law in law enforcement activities: a comparative legal study

Abstract: The article presents a comparative analysis of current approaches to the application of artificial intelligence (AI) in the sphere of control and supervisory activities by law enforcement agencies of foreign countries and Russia. The object of the study is normative acts, recommendations and other documents regulating the application of artificial intelligence in law enforcement, judicial practice, academic publications and analytical reports on the researched problem.

The research methodology integrates a set of modern philosophical, general scientific, special scientific methods of cognition, including dialectical, systemic, structural-functional, hermeneutic, comparative-legal, formal-legal (dogmatic) and others.

The study focuses on the implementation of a comparative legal study of the areas of application of AI in law enforcement. The research focuses on the development of unified approaches to regulating the use of AI and countering AI used in unlawful activities.

The results of the comparative analysis revealed basic problems in the field of ensuring the accuracy of analytical tools used in the investigation of crimes and suppression of offences; considered theoretical and practical situations of application of artificial intelligence in law enforcement; studied some examples of deepfake technology application in illegal activities and mechanisms of counteraction to this technology.

The author suggested additional compensatory legal measures to ensure the effective integration of artificial intelligence and its use for the purposes of law enforcement agencies of Russia.

Keywords: artificial intelligence, comparative legal research, predictive law, public law, law enforcement practice

For citation: Atabekov A. R. Issues in the implementation of predictive law in law enforcement activities: a comparative legal study // Vestnik of St. Petersburg University of the Ministry of Internal Affairs of Russia. – 2023. – № 3 (99). – P. 67–75; doi: 10.35750/2071-8284-2023-3-67-75.

Введение

Большинство стран мира (США[1], ФРГ[2], КНР[3] и т. д.), ОЭСР[4], в том числе Россия, видят своей приоритетной целью разработку и совершенствование регулятивных подходов в отношении ИИ на стратегическом уровне и на уровне отдельных законодательных инициатив 2021 года (в случае с Европейским союзом)[5].

Значимость правового регулирования ИИ в России прямо закреплена Указом Президента Российской Федерации В. В. Путина, где был определён основной стратегический вектор развития данной технологии и вектор необходимого правового режима для функционирования ИИ[6].

Следует также отметить, что Президент России неоднократно упоминал значимость

[1] Стратегические документы [Электронный ресурс] // Национальный офис инициативы искусственного интеллекта : сайт. – URL: https://www.ai.gov/strategy-documents/ (дата обращения: 20.06.2023).

[2] Künstliche Intelligenz (KI) ist ein Schlüssel zur Welt von morgen Strategie [Электронный ресурс] // Die Bundesregierung : сайт. – URL: https://www.ki-strategie-deutschland.de/ (дата обращения: 20.06.2023).

[3] Государственный совет по печати и распространению. Уведомление о Плане развития искусственного интеллекта нового поколения (2017) [Электронный ресурс] // Gov.cn : сайт. – URL: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm (дата обращения: 20.06.2023).

[4] Политика, данные и анализ для надежного искусственного интеллекта [Электронный ресурс] // AI General Dashboard. (OECD) : сайт. – URL: https://oecd.ai/en/dashboards/ (дата обращения: 20.06.2023).

[5] Proposal for a Regulation laying down harmonised rules on artificial intelligence [Электронный ресурс] // AI Act: сайт. – URL: https://ec.europa.eu/newsroom/dae/redirection/document/75788 / (дата обращения: 22.06.2023).

[6] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»)» [Электронный ресурс] // Доступ из СПС КонсультантПлюс: сайт. – URL : https://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 20.06.2023).

данной технологии для страны на конференциях, посвящённых ИИ, в течение 2022 года[7, 8].

При этом в правоохранительной деятельности ИИ является одним из значимых инструментов как для расследования преступлений (в рамках УК РФ), так и для пресечения потенциальных правонарушений (в рамках КоАП РФ).

В связи с этим нельзя не отметить выступление Генерального прокурора Российской Федерации в рамках ПМЭФ 2023 года, где была отмечена роль вновь созданного подразделения, занимающегося ИИ для целей прогнозирования противоправной деятельности[9] .

Изложенное выше позволяет говорить об актуальности проблемы, которая исследуется в настоящей статье.

Методы

Методологическая основа исследования представлена комплексом современных философских, общенаучных, специально-научных методов познания, включая диалектический, системный, структурно-функциональный, герменевтический, сравнительно-правовой, формально-юридический (догматический), метод правового моделирования и др.

В настоящей статье делается акцент на осуществлении сравнительного правового исследования подходов в области регулирования и регламентации применения ИИ в правоохранительной и публичной сфере по опыту иностранных государств и России.

Дополнительно в настоящей статье обращается особое внимание на герменевтический метод при исследовании правовых подходов для регламентации применения ИИ в области частноправовых и публичных правоотношений с учётом законодательных и судебных актов.

Кроме того, использован метод моделирования правового регулирования ИИ с последующей выработкой регламентирующих подходов для обеспечения баланса интересов при осуществлении правоохранительной деятельности с учётом наличия инструментов совершения правонарушений на базе той же технологии.

Результаты

Рассматривая составные элементы ИИ, необходимо отметить два базовых элемента, которые уже активно используются в правоохранительной деятельности (как при расследовании преступлений, так и в рамках административных процедур при пресечении правонарушений).

Одним из элементов является компьютерное зрение, которое позволяет на базе технических алгоритмов интерпретировать окружающую среду [1, с. 1]. Данная технология активно используется как в рамках контроля дорожного движения, так и для дополнительного анализа местонахождения субъектов или объектов посредством наружных средств наблюдения [2, с. 3400–3401]. При этом необходимо отметить, что в контексте полноценного формирования ИИ для целей правоохранительной деятельности заметную роль играет машинное обучение, когда система может обучаться и совершенствоваться без участия человека [3].

Следует отметить, что в научной среде вопрос качества и влияния прогнозистики для правоохранительной деятельности является одним из самых перспективных направлений и имеет давнюю историю как в России [4], так и за рубежом (Национальный институт юстиции (NIJ) [5], полицейские управления США [6] и т. д.).

При этом необходимо отметить, что методы обхода средств наблюдения, практикуемые правонарушителями и преступниками, также постоянно совершенствуются и требуют соответствующей реакции со стороны органов власти. Так, необходимо активнее использовать возможности определения местоположения правонарушителя при помощи вышек сотовой связи, передвижных камер на базе дронов с последующей интеллектуальной аналитикой [7]. Однако при этом возникают как технические, так и фундаментальные правовые вопросы о допустимости и возможности использования указанных технологий.

Среди технических возникает вопрос допустимой высоты и зоны покрытия указанной технологии, а среди правовых вопросов – порядок обработки большого количества персональных данных, их хранения, интерпретации, в т. ч. в контексте недопустимости нарушения базовых правовых интересов общества [8, с. 78].

Отметим, что практика применения сотрудниками полиции нательных камер предоставляет возможность применения данного подхода на полностью автономной основе.

Говоря о потенциальных технологиях ИИ для правоохранительной деятельности и их эффективности, необходимо обратиться к решениям Waikato Environment for Knowledge Analysis (WEKA) [9, с. 82–83]. Изначально крайне низкая эффективность прогнозистики, построенной на исторических данных о преступлениях и правонарушениях с 2003 по 2018 год, составляла 39–44 % [10, с. 7–8]. За счёт добавления дополнительных инструментов нейронных сетей, оценки плотности ядра и опорных векторов, точность моделирования достигла 67 % для последних двух инструментов и более 84 % для нейронных сетей [11, с. 1405–1408].

При этом многие представители научного сообщества, являющиеся практиками, задей-

---

[7] Президент принял участие в основной дискуссии международной конференции по искусственному интеллекту и машинному обучению Artificial Intelligence Journey 2022 на тему «Технологии искусственного интеллекта для обеспечения экономического роста» [Электронный ресурс] // Президент России: сайт. – URL: http://kremlin.ru/events/president/news/69927 (дата обращения: 22.06.2023).

[8] Владимир Путин выступил на расширенном заседании коллегии Министерства обороны, состоявшемся в Национальном центре управления обороной на Фрунзенской набережной [Электронный ресурс] // Kremlin.ru : сайт. – URL: http://kremlin.ru/events/president/news/70159 (дата обращения: 22.06.2023).

[9] ГП стала применять искусственный интеллект для прогнозирования ситуации с преступностью [Электронный ресурс] // Tass.ru : сайт. – URL: https://tass.ru/obschestvo/18042003 (дата обращения: 20.06.2023).

ствованными в решении вопроса прогнозирования правонарушений, пытаются разработать более точные инструменты прогнозистики [12], которые изначально обеспечили точность прогноза 66 % при условии таких упущенных параметров, как масштабируемость, долговечность и отказоустойчивость [13; 14] и т. д.

Д. Патель и др. смогли предсказать место совершения преступления с точностью в 87 %, однако такая точность не обеспечивается при большой выборке данных, т. е. не может использоваться в городах-миллионниках [15, с. 14–16].

В. Б. Батоев, исследовавший правовой аспект регламентации применения больших массивов данных в оперативно-розыскной деятельности, отмечает отсутствие законодательно закреплённых принципов и подходов применения таких данных в контексте предиктивной аналитики и преследования, необходимость совершенствования Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ, пересмотра подходов в области допуска к ограниченной информации (с учётом постоянного прогресса в области ИТ) [16, с. 14–17].

А. П. Суходолов и др. считают одной из практических проблем использования предиктивных инструментов анализа тот факт, что многие данные о криминологической обстановке хранятся на бумажных носителях и не интегрируются с сетевыми базами данных правоохранительных органов [17, с. 722].

Р. И. Дремлюга и В. В. Решетников в сравнительно-правовом исследовании применения ИИ для предиктивной аналитики, используемой правоохранительными органами, отмечают, что интересной и жизнеспособной конструкцией, позволяющей пресекать правонарушения, является убеждение лиц в необходимости отказаться от совершения преступлений. Данный подход является развитием конструкции, заложенной в ст. 31 УК РФ [18, с. 141–142].

Е. В. Никитин отмечает эффективность применения IT-технологий правоохранительными органами для обеспечения правопорядка при проведении Чемпионата мира по футболу в 2018 году (видеоанализ и прогнозистика) и обосновывает необходимость использования метода анализа иерархий для целей правоохранительной деятельности [19, с. 58].

Н. В. Павличенко и А. И. Тамбовцев рассматривают текущий феномен прогнозистики и необходимости работы с большим объёмом данных в целях развития кадрового потенциала правоохранительных органов с последующей актуализацией стандартов и программ подготовки специалистов для правоохранительной системы [20, с. 67].

Следующим перспективным направлением является использование биометрических методов на базе ИИ, заменяющих методы ручной идентификации в криминалистике [21].

Однако следует иметь в виду, что сверка биометрических данных лица, медицинских анализов и т. д. путём потоковой алгоритмической обработки запрещена как в ЕС (Директива 2016/6803[10]), так и в России (ст. 16 ФЗ[11]).

Учитывая опыт регламентации данных правоотношений в ЕС, научное сообщество обращает внимание на отсутствие ясности в отношении юридических требований, касающихся автоматизированной обработки персональных биометрических данных [22, с. 533–537].

Рассматривая технические аспекты применения алгоритмического анализа биометрических и биологических данных, необходимо отметить, что должны учитываться и такие факторы, как выражение лица, поза, сам датчик, условия фиксации, окружающая среда, порядок взаимодействия с датчиком, контрольные сверки данных в различных условиях [23; 24].

Кроме того, также нужно принимать во внимание старение организма, его возможные физические изменения (от наружных показателей – таких как волосяная растительность, до изменения веса и иных параметров тела).

Говоря о порядке фиксации видеоизображения, важно учесть и технические аспекты – к примеру, разрешение изображения для надёжной идентификации объекта по чертам лица [25, с. 323–325] или слишком большое расстояние до объекта.

Нельзя не упомянуть и такую технологию, как «Deepfake», базирующуюся на методах глубокого обучения и «фейков» (подделках данных, вывода информации и т. п.) [26]. Эта программа способна самообучаться, в т. ч. на базе постоянно генерируемых и состязающихся между собой сетей. Впервые эту технологию использовали в 2017 году, когда с её помощью лицо актрисы интимного характера было заменено на лицо знаменитости [27, с. 1308].

Следует отметить, что «Deepfake» становится доступной и для технически неподготовленных людей, что ведёт к кратному увеличению поддельной аудио- и видеопродукции. При этом изготовление и распространение материалов интимного характера с подменой лица пользователя является далеко не самым опасным вариантом применения этой программы.

Так, в марте 2021 года Народная прокуратура района Хункоу муниципалитета Шанхая в Китае возбудила уголовное дело по факту предоставления поддельной счёт-фактуры с указанием недостоверных данных НДС. В рамках прохождения видеоверификации подозреваемый подделывал видеоролики с имитацией кивания и т. д., для выставления ложных счёт-фактур для последующей манипуляции с уплатой НДС [27, с. 1310].

---

[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 [Электронный ресурс] // Eur-lex : сайт. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680 (дата обращения: 20.06.2023).

[11] Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» [Электронный ресурс] // Доступ из СПС КонсультантПлюс: сайт. – URL : https://www.consultant.ru/document/cons_doc_LAW_61801/22e884a41450dcb5cb62d956583ad32abe2bbbe9/ (дата обращения: 20.06.2023).

В 2018 году более двадцати человек в Индии были убиты из-за ложных сообщений, разосланных через мессенджер WhatsApp, о похищении маленьких детей или других преступлениях, якобы совершенных ими[12].

Пока данные феномены носят относительно абстрактный характер, однако если мы рассмотрим функционирование технологии через призму «e-justice», когда происходит рассмотрение судебного дела (гражданского, административного и некоторых составов применительно к уголовным делам) в формате онлайн-видеотрансляции, то отсутствие контроля за указанной технологией со стороны профильных органов власти и правоохранительных органов вызывает существенные опасения.

На уровне законодательной ветви власти нельзя не отметить политические дипфейки, имевшие место в президентской компании в США в 2020 году[13], дипломатии[14] и т. д.

Рассматривая регулятивные подходы противодействия дипфейкам, необходимо отметить опыт США, ЕС и Китая.

Представители органов власти и законодательной ветви власти США достаточно оперативно отреагировали на подобное недобросовестное применение ИИ. В декабре 2018 г. Конгресс США принял запрет на использование противоправных дипфейков[15], который был первым законом в мире, определяющим параметры и правовую природу дипфейка. Отдельно в июне 2019 г. был принят закон об ответственности за использование вышеуказанной технологии[16]. В том же году Конгресс обязал Службу национальной безопасности регулярно готовить отчёты с оценкой преступной активности указанной технологии[17].

Данные инициативы относятся к федеральному уровню, но и на уровне штатов принято немало дополняющих актов, например в Калифорнии[18], Вашингтоне[19], Нью-Йорке[20] и т. д.

Рассматривая инструменты противодействия дипфейку в ЕС, необходимо отметить, что специальное законодательство (как это было в США) ЕС не разрабатывал, однако принял ряд дополнений и уточнений в действующее законодательство, в т. ч. в контексте общей регламентации ИИ.

В апреле 2018 года Европейская комиссия опубликовала манифест «Борьба с дезинформацией в интернете», определивший общеевропейский подход к этому негативному явлению, не допускающий использования изданий, незаконно манипулирующих общественным мнением[21]. В мае того же года ЕС официально внедрил Общие положения о защите данных. В рамках указанного документа установлены существенные императивные конструкции, ограничивающие порядок применения глубоких технологий синтеза и воспроизводства данных, связанных с личностью человека (лицо, голос и т. д.), а также общие принципы защиты персональных данных, которые в той или иной мере могут быть использованы ИИ для создания дипфейков [28].

Китай также не использует специального регулирования в отношении технологии дипфейка.

Базовым инструментом в отношении общей технологии ИИ является издание стандартов и ограничение на создание, публикацию и распространение недостоверной информации о личности[22], с точки зрения защиты персональных прав граждан (их персональные данные и репутация[23]). Кроме того, искусственно созданные или воспроизведённые портреты подвергаются обязательной маркировке[24].

---

[12] Donie O'Sullivan. House Intel chair sounds alarm in Congress' first hearing on deepfake videos [EB/OL]: [Электронный ресурс] // Edition.cnn.com: сайт. – URL : https://edition.cnn.com/2019/06/13/tech/deepfakecongress-hearing/index. html (дата обращения: 20.06.2023).

[13] Generally 'FBI Chief Calls Capitol Attack Domestic Terrorism and Rejects Trump's Fraud Claims' [Электронный ресурс] // The Guardian: сайт. – URL: https://www.theguardian.com/usnews/2021/jun/10/capitol-attackfbi-christopherwray-congress (дата обращения: 20.06.2023).

[14] Krishnadev Calamur, Did Russian Hackers Target Qatar? [Электронный ресурс] // The atlantic : сайт. – URL: https: //www.theatlantic.com/news/archive/2017/06 / Qatar-russian-hacker-fake-news/529359/ (дата обращения: 20.06.2023).

[15] S.3805 – Malicious Deep Fake Prohibition Act of 2018 [Электронный ресурс] // Www.congress.gov : site. – URL : https://www.congress.gov/bill/115th-congress/senate-bill/3805 (дата обращения: 20.06.2023).

[16] H.R.3230-Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2019 [Электронный ресурс] / /Www.congress.gov : site. – URL : http://www.congress.gov/bill/116th -congress/house-bill/3230 (дата обращения: 20.06.2023).

[17] Deepfakes Report Act of [Электронный ресурс] // Www.congress.gov : site. – URL : https://www.congress.gov/bill/116thcongress/house-bill/3600/ (дата обращения: 20.06.2023).

[18] Depiction of individual using digital or electronic technology: sexually explicit material: cause of action [Электронный ресурс] // Openstates : site. – URL : https://openstates.org/ca/bills/20192020/AB602/ (дата обращения: 20.06.2023).

[19] Washington State Passes Law Restricting Use of Facial Recognition Services [Электронный ресурс] // Hunton Andrews Kurth : site. – URL : https://www.huntonprivacyblog.com/2020/03/20/washington-state-passes-law-restricting-use-of-facial-recognition-services/ (дата обращения: 20.06.2023).

[20] New York Assembly Bill 8155 [Электронный ресурс] // Legiscan.com : site. – URL : https://legiscan.com/NY/text/A08155/id/1805616 (дата обращения: 20.06.2023).

[21] European Commission. Tackling Online Disinformation: A European Approach[J]. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM/2018/236, 2018 [Электронный ресурс] // Lex.europa : site. – URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:794:FIN (дата обращения: 20.06.2023).

[22] Administrative Regulations on Online Audio and Video Information Services [Электронный ресурс] // CLP : site. – URL : https://www.chinajusticeobserver.com/law/x/online-audio-and-video-information-services-20191118 (дата обращения: 20.06.2023).

[23] Civil Code of the People's Republic of China [Электронный ресурс] // Gov.cn : site. – URL : http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf (дата обращения: 20.06.2023).

[24] Order of the Cyberspace Administration of China [Электронный ресурс] // Wilmap: site. – URL : https://wilmap.stanford.edu/entries/provisions-governance-online-information-content-ecosystem (дата обращения: 20.06.2023).

Что касается России, необходимо отметить позицию отечественных юристов и практиков в области противодействия технологии «дипфейк».

Так, Г. И. Миняшева полагает, что в нашей стране эта проблема урегулирована лишь частично. Вопросы, связанные с созданием и использованием дипфейков, подпадают под санкции ст. 159 УК РФ и ст. 152 ГК РФ [29, с. 194–195].

М. А. Желудков в своей статье отмечает, что практика расследований преступлений, особенно с использованием IT-технологий, требует формирования новых правовых форм, в т. ч. для защиты интересов общества от противоправного применения технологии «дипфейк». Данная ситуация требует пересмотра не только положений УПК РФ (ст. 75), но и нормативных актов, касающихся использования биометрических данных человека [30, с. 269].

Схожую позицию занимает Л. Югай. В рамках проведённого ею исследования она отмечает, что возможными мерами по противодействию мошенничества с использованием биометрии может выступить как формирование дополнительных инструментов верификации личности, так и разработка Концепции национальной системы биометрической идентификации личности [31, с. 62].

О. В. Расторопова пишет, что возможным оптимальным инструментом противодействия противоправному применению ИИ может выступить кооперация органов власти в формате государственно-частного партнёрства, с учётом аналогичного опыта США (IBM Watson) [32].

С. В. Лемайкина говорит о необходимости своевременного и добросовестного информирования сотрудниками ОВД граждан о дискредитации пользователей посредством технологии «дипфейк», а также обязательного повышения квалификации сотрудников правоохранительной сферы в области информационной безопасности [33, с. 177].

Комплексный правовой подход сдерживания и противодействия дипфейк-технологии представил А. Г. Карпика, обозначив необходимость правовой фиксации понятия «поддельное цифровое изображение личности», введения ответственности за использование указанной личности (в рамках административного и уголовного права), совершенствование криминалистического исследования с помощью выявления технических уязвимостей при анализе изображений [34, с. 112–113].

Заключение

На основании вышеизложенного можно сделать следующие выводы.

1. Точность прогнозистики правонарушений требует всё большего количества персональных данных, в т. ч. и таких, которые могут затрагивать базовые права человека, в рамках анализа больших массивов данных (big-data) технологией ИИ.

2. В случае развития инструментов предиктивного преследования необходимо определить правовой консенсус между общественной безопасностью и личными правами.

3. В рамках определения указанной конструкции потребуются существенные новеллы в действующие КоАП РФ, УПК РФ и т. д., определяющие как правовой статус используемой технологии, условия её использования, так и прямо фиксирующие зоны ответственности разработчика, пользователя и самой технологии (с возможным выделением отдельной правосубъектности [35, с. 50]).

4. Открытым останется вопрос определения момента потенциального совершения правонарушения, его квалификации и последующего привлечения к ответственности с учётом пересечения большинства составов в рамках КоАП РФ и УК РФ, учитывая, что на момент потенциального совершения правонарушения квалификация может быть «плавающая».

5. В рамках предиктивного преследования открытым вопросом остаётся также применение оповещающих инструментов (Госуслуг) о потенциальной интерпретации действий лица в рамках проведённого наружного анализа, сверки с биометрической базой данных и иных публичных и открытых сервисов или сервисов, которые используются правоохранительными органами.

6. Необходимо выработать алгоритм идентификации правонарушений, а также ужесточить ответственность за применение ИИ, в т. ч. посредством технологии «дипфейк» (но не ограничиваясь только ею) в противоправных действиях, предусмотренных КоАП РФ и УК РФ.

Список литературы

1. *William P., Badholia A.* Analysis of personality traits from text-based answers using HEXACO model // 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). – IEEE, 2021. – С. 1–10.

2. *William P., Badholia A.* Evaluating Efficacy of Classification Algorithms on Personality Prediction Dataset // Elementary Education Online. – 2020. – Т. 19. – № 4. – С. 3400–3413.

3. *Bibave R. et al.* A Comparative Analysis of Single Phase to Three Phase Power Converter for Input Current THD Reduction //2022 International Conference on Electronics and Renewable Systems (ICEARS). – IEEE, 2022. – С. 325–330.

4. *Агамиров К. В.* Проблемы юридического прогнозирования: методология, теория, практика : монография / под науч. ред. Р. В. Шагиевой. – Москва: Юркомпани, 2015. – 406 с. – (Серия «Актуальные юридические исследования»).

5. *Go A. et al.* Twitter sentiment analysis // Entropy. – 2009. – Т. 17. – 252 с.

6. *Lima A. C. E. S., de Castro L. N.* Automatic sentiment analysis of Twitter messages / 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN). – IEEE, 2012. – С. 52–57.

7. *Vedaldi A., Fulkerson B.* VLFeat: An open and portable library // Computer Vision Algorithms. ACMMM. – 2010. – С. 1469–1472. https://doi.org/10.1145/1873951.1874249.

8. *Мавринская Т. В., Лошкарёв А. В., Чуракова Е. Н.* Обезличивание персональных данных и технологии «больших данных» (BigData) // Интерактивная наука. – 2017. – № 16. – С. 78–80.

9. *Pathan M. et al.* Artificial cognition for applications in smart agriculture: A comprehensive review // Artificial Intelligence in Agriculture. – 2020. – Т. 4. – С. 81–95.

10. *Pandya R. et al.* Buildout of methodology for meticulous diagnosis of K-complex in EEG for aiding the detection of Alzheimer's by artificial intelligence // Augmented Human Research. – 2020. – Т. 5. – С. 1–8. DOI: 10.1007/s41133-019-0021-6.

11. *Musumeci F. et al.* An overview on application of machine learning techniques in optical networks // IEEE Communications Surveys & Tutorials. – 2018. – Т. 21. – № 2. – С. 1383–1408.

12. *Judd J. S.* Learning in networks is hard // Proc. of 1st International Conference on Neural Networks, San Diego, California, June 1987. – IEEE, 1987.

13. *Panchiwala S., Shah M.* A comprehensive study on critical security issues and challenges of the IoT world //Journal of Data, Information and Management. – 2020. – Т. 2. – С. 257–278.

14. *Simon A. et al.* An overview of machine learning and its applications //International Journal of Electrical Sciences & Engineering. – 2016. – Т. 1. – № 1. – С. 22–24.

15. *Patel D., Shah D., Shah M.* The intertwine of brain and body: a quantitative analysis on how big data influences the system of sports //Annals of Data Science. – 2020. – Т. 7. – С. 1–16.

16. *Батоев В. Б.* «Большие данные (Big Data)» и предиктивная аналитика в оперативно-разыскной деятельности: проблемы использования и пути решения // Вестник Волгоградской академии МВД России. – 2020. – № 1 (52). – С. 11–17.

17. *Суходолов А. П. и др.* Big data как современный криминологический метод изучения и измерения организованной преступности // Всероссийский криминологический журнал. – 2019. – Т. 13. – № 5. – С. 718–726.

18. *Дремлюга Р. И., Решетников В. В.* Правовые аспекты применения предиктивной аналитики в правоохранительной деятельности // Азиатско-Тихоокеанский регион: экономика, политика, право. – 2018. – Т. 20. – № 3. – С. 133–144.

19. *Никитин Е. В.* О новых возможностях применения современных цифровых технологий в правоохранительной деятельности // Правопорядок: история, теория, практика. – 2018. – № 4 (19). – С. 55–59.

20. *Павличенко Н. В., Тамбовцев А. И.* Будущее профессии оперуполномоченный – Big Data и аналитика // Труды академии управления МВД России. – 2020. – № 2 (54). – С. 62–68.

21. *Saini M., Kapoor A. K.* Biometrics in forensic identification: applications and challenges // J Forensic Med. – 2016. – Т. 1. – № 108. – С. 2. DOI: 10.4172/2472-1026.1000108.

22. *Kindt E. J.* Having yes, using no? About the new legal regime for biometric data // Computer law & security review. – 2017. – Т. 34. – № 3. – С. 523–538. DOI:10.1016/j.clsr.2017.11.004.

23. *Tistarelli M., Grosso E., Meuwly D.* Biometrics in forensic science: challenges, lessons and new technologies //Biometric Authentication: First International Workshop, BIOMET 2014, Sofia, Bulgaria, June 23–24, 2014. Revised Selected Papers 1. – Springer International Publishing, 2014. – С. 153–164. DOI:10.1007/978-3-319-13386-7_12.

24. *Zeinstra C. G. et al.* Forensic face recognition as a means to determine strength of evidence: a survey // Forensic Sci Rev. – 2018. – Т. 30. – № 1. – С. 21–32.

25. *Bouchrika I.* Evidence evaluation of gait biometrics for forensic investigation //Multimedia Forensics and Security: Foundations, Innovations, and Applications. – 2017. – С. 307–326. DOI: 10.1007/978-3-319-44270-9_13.

26. *Brandon J.* Terrifying high-tech porn: creepy'deepfake'videos are on the rise // Fox news. – 2018. – Т. 20 [Electronic resource] // FoxNews : site – URL: https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise (date of treatment: 03.05.2023).

27. *Liu M., Zhang X.* Deepfake Technology and Current Legal Status of It //2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022). – Atlantis Press, 2022. – С. 1308–1314. DOI: 10.2991/978-94-6463-040-4_194.

28. *Voigt P., Von dem Bussche A.* The eu general data protection regulation (gdpr) // A Practical Guide, 1st Ed., Cham: Springer International Publishing. – 2017. – Т. 10. – № 3152676. – 383 с. https://doi.org/10.1007/978-3-319-57959-7.

29. *Миняшева Г. И.* Выявление и раскрытие мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий / Современные проблемы уголовного процесса: пути решения сборник материалов 3-й Международной конференции / под общей ред. А. Ю. Терехова. – Уфа: Издательство Уфимского юридического института МВД России, 2022. – С. 191–197.

30. *Желудков М. А.* Изучение влияния новых цифровых технологий на детерминацию мошеннических действий (технология deepfake) / Развитие наук антикриминального цикла в свете глобальных вызовов обществу : сборник трудов по материалам Всероссийской заочной научно-практической конференции с международным участием. – Саратов, 2021. – С. 262–270.

31. *Югай Л. Ю.* Мошенничество с использованием биометрических технологий: сущность, риски и меры противодействия // Правовые вопросы противодействия мошенничеству и киберпреступлениям. – 2021. – Т. 1. – № 1. – С. 59–63.

32. *Расторопова О. В.* Противодействие использованию искусственного интеллекта в преступных целях // Вестник Университета прокуратуры Российской Федерации. – 2021. – Т. 4. – № 84. – С. 52–58.

33. *Лемайкина С. В.* Актуальные вопросы противодействия использованию технологии дипфейков // Юристъ-Правоведъ. – 2022. – № 3 (102). – С. 175–178.

34. *Карпика А. Г.* Актуальные вопросы совершенствования правового и технического обеспечения противодействия преступлениям, совершаемым с использованием технологий искусственного интеллекта // Философия права. – 2021. – № 3 (98). – С. 109–113.

35. *Ястребов О. А.* Правосубъектность электронного лица: теоретико-методологические подходы // Труды Института государства и права Российской академии наук. – 2018. – Т. 13. – № 2. – С. 36–55.

References

1. *William P., Badholia A.* Analysis of personality traits from text-based answers using HEXACO model // 2021 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES). – IEEE, 2021. – S. 1–10.

2. *William P., Badholia A.* Evaluating Efficacy of Classification Algorithms on Personality Prediction Dataset // Elementary Education Online. – 2020. – T. 19. – № 4. – S. 3400–3413.

3. *Bibave R. et al.* A Comparative Analysis of Single Phase to Three Phase Power Converter for Input Current THD Reduction //2022 International Conference on Electronics and Renewable Systems (ICEARS). – IEEE, 2022. – S. 325–330.

4. *Agamirov K. V.* Problemy yuridicheskogo prognozirovaniya: metodologiya, teoriya, praktika : monografiya / pod nauch. red. R. V. Shagiyevoy. – Moskva: Yurkompani, 2015. – 406 s. – (Seriya «Aktual'nyye yuridicheskiye issledovaniya»).

5. *Go A. et al.* Twitter sentiment analysis // Entropy. – 2009. – T. 17. – 252 s.

6. *Lima A. C. E. S., de Castro L. N.* Automatic sentiment analysis of Twitter messages / 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN). – IEEE, 2012. – S. 52–57.

7. *Vedaldi A., Fulkerson B.* VLFeat: An open and portable library // Computer Vision Algorithms. ACMMM. – 2010. – S. 1469–1472. https://doi.org/10.1145/1873951.1874249.

8. *Mavrinskaya T. V., Loshkarov A. V., Churakova Ye. N.* Obezlichivaniye personal'nykh dannykh i tekhnologii «bol'shikh dannykh» (BigData) // Interaktivnaya nauka. – 2017. – № 16. – S. 78–80.

9. *Pathan M. et al.* Artificial cognition for applications in smart agriculture: A comprehensive review // Artificial Intelligence in Agriculture. – 2020. – T. 4. – S. 81–95.

10. *Pandya R. et al.* Buildout of methodology for meticulous diagnosis of K-complex in EEG for aiding the detection of Alzheimer's by artificial intelligence // Augmented Human Research. – 2020. – T. 5. – S. 1–8. DOI: 10.1007/s41133-019-0021-6.

11. *Musumeci F. et al.* An overview on application of machine learning techniques in optical networks // IEEE Communications Surveys & Tutorials. – 2018. – T. 21. – № 2. – S. 1383–1408.

12. *Judd J. S.* Learning in networks is hard // Proc. of 1st International Conference on Neural Networks, San Diego, California, June 1987. – IEEE, 1987.

13. *Panchiwala S., Shah M.* A comprehensive study on critical security issues and challenges of the IoT world //Journal of Data, Information and Management. – 2020. – T. 2. – S. 257–278.

14. *Simon A. et al.* An overview of machine learning and its applications //International Journal of Electrical Sciences & Engineering. – 2016. – T. 1. – № 1. – S. 22–24.

15. *Patel D., Shah D., Shah M.* The intertwine of brain and body: a quantitative analysis on how big data influences the system of sports //Annals of Data Science. – 2020. – T. 7. – S. 1–16.

16. *Batoyev V. B.* «Bol'shiye dannyye (Big Data)» i prediktivnaya analitika v operativno-razysknoy deyatel'nosti: problemy ispol'zovaniya i puti resheniya // Vestnik Volgogradskoy akademii MVD Rossii. – 2020. – № 1 (52). – S. 11–17.

17. *Sukhodolov A. P. i dr.* Big data kak sovremennyy kriminologicheskiy metod izucheniya i izmereniya organizovannoy prestupnosti // Vserossiyskiy kriminologicheskiy zhurnal. – 2019. – T. 13. – № 5. – S. 718–726.

18. *Dremlyuga R. I., Reshetnikov V. V.* Pravovyye aspekty primeneniya prediktivnoy analitiki v pravookhranitel'noy deyatel'nosti // Aziatsko-Tikhookeanskiy region: ekonomika, politika, pravo. – 2018. – T. 20. – № 3. – S. 133–144.

19. *Nikitin Ye. V.* O novykh vozmozhnostyakh primeneniya sovremennykh tsifrovykh tekhnologiy v pravookhranitel'noy deyatel'nosti // Pravoporyadok: istoriya, teoriya, praktika. – 2018. – № 4 (19). – S. 55–59.

20. *Pavlichenko N. V., Tambovtsev A. I.* Budushcheye professii operupolnomochennyy – Big Data i analitika // Trudy akademii upravleniya MVD Rossii. – 2020. – № 2 (54). – S. 62–68.

21. *Saini M., Kapoor A. K.* Biometrics in forensic identification: applications and challenges // J Forensic Med. – 2016. – T. 1. – № 108. – S. 2. DOI: 10.4172/2472-1026.1000108.

22. *Kindt E. J.* Having yes, using no? About the new legal regime for biometric data // Computer law & security review. – 2017. – Т. 34. – № 3. – S. 523–538. DOI:10.1016/j.clsr.2017.11.004.

23. *Tistarelli M., Grosso E., Meuwly D.* Biometrics in forensic science: challenges, lessons and new technologies //Biometric Authentication: First International Workshop, BIOMET 2014, Sofia, Bulgaria, June 23–24, 2014. Revised Selected Papers 1. – Springer International Publishing, 2014. – S. 153–164. DOI:10.1007/978-3-319-13386-7_12.

24. *Zeinstra C. G. et al.* Forensic face recognition as a means to determine strength of evidence: a survey // Forensic Sci Rev. – 2018. – Т. 30. – № 1. – S. 21–32.

25. *Bouchrika I.* Evidence evaluation of gait biometrics for forensic investigation //Multimedia Forensics and Security: Foundations, Innovations, and Applications. – 2017. – S. 307–326. DOI: 10.1007/978-3-319-44270-9_13.

26. *Brandon J.* Terrifying high-tech porn: creepy'deepfake'videos are on the rise // Fox news. – 2018. – Т. 20 [Electronic resource] // FoxNews : site – URL: https://www.foxnews.com/tech/terrifying-high-tech-porn-creepy-deepfake-videos-are-on-the-rise (date of treatment: 03.05.2023).

27. *Liu M., Zhang X.* Deepfake Technology and Current Legal Status of It //2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022). – Atlantis Press, 2022. – S. 1308–1314. DOI: 10.2991/978-94-6463-040-4_194.

28. *Voigt P., Von dem Bussche A.* The eu general data protection regulation (gdpr) // A Practical Guide, 1st Ed., Cham: Springer International Publishing. – 2017. – Т. 10. – № 3152676. – 383 s. https://doi.org/10.1007/978-3-319-57959-7.

29. *Minyasheva G. I.* Vyyavleniye i raskrytiye moshennichestv, sovershayemykh s ispol'zovaniyem informatsionno-telekommunikatsionnykh tekhnologiy / Sovremennyye problemy ugolovnogo protsessa: puti resheniya sbornik materialov 3-y mezhdunarodnoy konferentsii / pod obshchey red. A. Yu. Terekhova. – Ufa: Izd-vo Ufimskogo yuridicheskogo instituta MVD Rossii 2022. – S. 191–197.

30. *Zheludkov M. A.* Izucheniye vliyaniya novykh tsifrovykh tekhnologiy na determinatsiyu moshennicheskikh deystviy (tekhnologiya deepfake) / Razvitiye nauk antikriminal'nogo tsikla v svete global'nykh vyzovov obshchestvu : sbornik trudov po materialam vserossiyskoy zaochnoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiyem. – Saratov, 2021. – S. 262–270.

31. *Yugay L. Yu.* Moshennichestvo s ispol'zovaniyem biometricheskikh tekhnologiy: sushchnost', riski i mery protivodeystviya // Pravovyye voprosy protivodeystviya moshennichestvu i kiberprestupleniyam. – 2021. – Т. 1. – № 1. – S. 59–63.

32. *Rastoropova O. V.* Protivodeystviye ispol'zovaniyu iskusstvennogo intellekta v prestupnykh tselyakh // Vestnik Universiteta prokuratury Rossiyskoy Federatsii. – 2021. – Т. 4. – № 84. – S. 52–58.

33. Lemaykina S. V. Aktual'nyye voprosy protivodeystviya ispol'zovaniyu tekhnologii dipfeykov // Yurist»-Pravoved». – 2022. – № 3 (102). – S. 175–178.

34. *Karpika A. G.* Aktual'nyye voprosy sovershenstvovaniya pravovogo i tekhnicheskogo obespecheniya protivodeystviya prestupleniyam, sovershayemym s ispol'zovaniyem tekhnologiy iskusstvennogo intellekta // Filosofiya prava. – 2021. – № 3 (98). – S. 109–113.

35. *Yastrebov O. A.* Pravosub»yektnost' elektronnogo litsa: teoretiko-metodologicheskiye podkhody // Trudy Instituta gosudarstva i prava Rossiyskoy akademii nauk. – 2018. – Т. 13. – № 2. – S. 36–55.

Статья поступила в редакцию 03.05.2023; одобрена после рецензирования 13.07.2023; принята к публикации 26.07.2023.

The article was submitted May 03, 2023; approved after reviewing July 13, 2023; accepted for publication July 26, 2023.