

АКТУАЛЬНЫЕ АСПЕКТЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ВНЕДРЕНИЯ ТЕХНОЛОГИЙ МАШИННОГО ОБУЧЕНИЯ

Сергей Владимирович Дейко^а

EDN: KUOJHG

^а Научно-исследовательский институт «Восход»

Аннотация: Статья посвящена изучению проблем правового обеспечения защиты персональных данных в условиях распространения технологий машинного обучения и связанных с ними систем искусственного интеллекта, нейронных сетей и блокчейн-технологий. Предметом статьи являются основные положения российского законодательства и юридической доктрины относительно актуальных аспектов использования технологий машинного обучения в контексте правовой защиты персональных данных. Тема исследования достаточно актуальна в свете меняющегося технологического облика современного общества. Российское законодательство должно совершенствоваться наряду с появлением новых инструментов, используемых для обработки персональных данных. Особенно это актуально для технологий машинного обучения, функционирование которых в силу новизны данного явления еще не в полной мере урегулировано соответствующими законодательными нормами. В статье продемонстрированы наиболее значимые аспекты использования технологий машинного обучения в рамках обработки конфиденциальных сведений, а также выявлены риски неправомерных посягательств на персональные данные. Автором отмечается необходимость конкретизации отдельных положений законодательства, которые должны учитывать специфику технологий машинного обучения, а также систем искусственного интеллекта, в алгоритмах которых могут быть использованы персональные данные о личности человека. В результате представлены варианты усовершенствования модели правового обеспечения защиты персональных данных и предложены конкретные законодательные решения в этой области.

Ключевые слова: машинное обучение, искусственный интеллект, нейронные сети, блокчейн, персональные данные

Дата поступления статьи в редакцию: 11 сентября 2024 года.

CURRENT ASPECTS OF PERSONAL DATA PROTECTION IN THE CONTEXT OF IMPLEMENTING MACHINE LEARNING TECHNOLOGIES

RESEARCH ARTICLE

Sergey V. Deiko^a

^a Scientific Research Institute Voskhod

Abstract: The goal of the article is to look at the legal issues surrounding personal data protection in the context of the widespread adoption of machine learning technologies, including artificial intelligence systems, neural networks, and blockchain technology. The article focuses on the key provisions of Russian legislation and legal theory governing contemporary application of machine learning technologies in the context of protecting private information. The focus of the study is particularly significant in light of modern society's changing technological landscape. Russian legislation must be modified to reflect the development of new technologies for processing personal data. Due to the novelty of this issue, the functioning of machine learning technologies has not yet been fully governed by pertinent regulatory rules, making the article especially relevant. It highlights the critical elements of using machine learning technology to handling confidential data and emphasizes the dangers of unlawful access to personal information. The author points out the necessity of defining particular legal requirements that should consider the peculiarities of artificial intelligence systems and machine learning technologies, whose algorithms may make use of personal information about individuals. The findings are reflected in the article's recommendations for strengthening the legal framework to protect personal data and its particular legislative adjustments.

Keywords: machine learning, artificial intelligence, neural networks, blockchain, personal data

Received: September 11, 2024.

Цифровая эпоха

Введение

Технологическое развитие общества, напрямую влияющее на содержание и характер течения общественных отношений, традиционно выступает одним из наиболее сильных стимулов для нормотворческой активности государственных органов, вынужденных оперативно реагировать на меняющийся облик взаимодействия субъектов права в условиях новой технологической реальности. Особенностью развития общественных отношений в последние годы является их форсированная цифровизация, сопровождающаяся устойчивым трендом на алгоритмизацию основных методов управленческого воздействия на поведение личности. Одним из наиболее впечатляющих технологических решений в области алгоритмизации публичного управления является внедрение технологий машинного обучения.

Данная технология является одной из форм технологического воплощения искусственного интеллекта, предполагающей возможность совершенствования в области решения типологически схожих задач. Это достигается за счет, прежде всего, использования нейросетей как программного и аппаратного воплощения математических моделей самообучения, имеющих безусловное превосходство перед традиционными алгоритмами. Вопрос о применении технологий машинного обучения в различных областях публичного управления был вопросом времени с самого момента их появления [Аюшеева, 2023. С. 128].

Нейронные сети, будучи инструментами машинного обучения, могут значительно улучшить качество обработки и анализа персональных данных, так как они способны выявлять скрытые закономерности в огромных объемах информации, что позволяет создавать более точные профили пользователей. Например, благодаря анализу персональных данных, таких как возраст, пол, местоположение и интересы, нейронные сети могут предлагать целенаправленную рекламу или персонализированные рекомендации, что повышает удовлетворенность клиентов и эффективность бизнес-процессов.

Анализ актуальных аспектов защиты персональных данных в условиях внедрения технологий машинного обучения опирается на применение ряда общенаучных и специально-юридических методов. В статье применяются диалектический, формально-логический, формально-юридический методы, а также метод правовой герменевтики. В качестве материалов используются нормативные положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

Правовое регулирование использования нейросетей, искусственного интеллекта и технологий машинного обучения

Внедрение нейросетей в различные области социальной жизни одновременно порождает соответствующие проблемы для механизма правового регулирова-

ния. С одной стороны, перед государством возникает задача разработки новых правотворческих решений, которые позволяли бы обеспечить необходимый уровень стандартизации форм и способов применения технологий машинного обучения. С другой стороны, привычные сферы общественных отношений также подвергаются модификации в условиях распространения практики использования нейросетей, что требует изменений в уже действующем законодательстве. Рассматриваемые технологии получают свое применение в самых разных сферах социального взаимодействия, которые подвергаются воздействию как средств частного правового, так и публично-правового характера [Литвин, 2021. С. 116].

Для области правового регулирования отношений, связанных с оборотом персональных данных, распространение технологий машинного обучения имеет несколько значимых последствий.

В первую очередь персональные данные затрагиваются разнообразными моделями искусственного интеллекта, которые могут быть использованы в компьютерных программах и приложениях для электронных мобильных устройств, собирающих и обрабатывающих конфиденциальные сведения. Кроме того, технологии машинного обучения могут быть элементом смарт-контрактов, которые применяются в качестве нового технологического решения при исполнении гражданско-правовых обязательств. В структуре таких договоров могут применяться технологии алгоритмизации исполнения обязательства в зависимости от совершения того или иного юридического действия, что может требовать программного обеспечения обработки поступающей информации на основе принципа самообучаемости информационной системы [Минбаев, Сторожакова, 2023. С. 75].

Технология блокчейн может помочь упростить процесс согласования и управления персональными данными. С помощью смарт-контрактов можно автоматизировать согласие на обработку данных, что минимизирует необходимость в сложных юридических процедурах. Пользователи смогут самостоятельно контролировать, какие именно данные они готовы предоставить и кому, используя децентрализованные приложения. Это создаст новый уровень взаимодействия между пользователями и организациями, где персональные данные станут управляемым и защищенным ресурсом, способствующим повышению уровня конфиденциальности сведений о личности человека [Свиридова, 2021. С. 65].

Такие практики использования современных технологических средств могут порождать определенные проблемы для правоприменения, так как законодательство не всегда результативным образом регулирует новые области внедрения машинного обучения. Во всех этих случаях возможны различные программные

методы обработки персональных данных, что формирует необходимость поиска эффективных юридических инструментов их защиты в условиях новой технологической реальности. Однако использование персональных данных также вызывает серьезные вопросы этического и правового характера. Сбор и обработка таких данных должны осуществляться в строгом соответствии с законодательством о защите данных, как, например, GDPR в Европе [Макаренко, 2022. С. 78].

Формирующиеся подходы в юридической доктрине в целом ориентированы на необходимость комплексного и взаимосвязанного рассмотрения проблем правового регулирования в сфере использования нейросетей, искусственного интеллекта и технологий машинного обучения. Хотя эти технологические феномены нельзя признать тождественными, их применение часто не позволяет провести четкую разделительную линию между ними. Юридическая природа использования новых технологических средств достаточно однообразна, а следовательно, на первоначальном этапе разработки научных проблем внедрения указанных технологий можно рассматривать как условно однородные. Рассмотрим основные проблемы правового регулирования защиты персональных данных в условиях использования технологий машинного обучения.

Первоочередной проблемой на пути дальнейшего развития законодательства в области защиты персональных данных является вопрос о правомерности алгоритмической обработки конфиденциальной информации при работе программных средств обеспечения функционирования персональных компьютеров и электронных мобильных устройств. Этот вид обработки информации типичен для ситуаций, при которых лица обращаются с запросом к системе машинного обучения (нейронной сети), когда работа этой технологии оказывается связанной с необходимостью предоставления доступа к конфиденциальной информации [Афанасьева, 2020. С. 44].

Поскольку направление запроса к системе, использующей технологии машинного обучения, как правило, осуществляется лицами на добровольной основе, то в такой ситуации может быть неуместным использование традиционных инструментов защиты персональных данных, таких как информированное согласие на их обработку. Если обработка таких сведений осуществляется нейронной сетью на автоматической основе, то этот вид применения технологий машинного обучения оказывается вне пространства действия принятых средств правового обеспечения защиты персональных данных [Новикова, 2024. С. 25].

Информационная система, использующая алгоритмы самообучения, лишь по аналогии может быть сопоставлена с известными законодательству технологическими решениями, в частности, базами данных, на работу которых распространяются классические

инструменты правовой охраны конфиденциальной информации. Ограниченность такой аналогии становится очевидной, когда речь заходит об имплементации персональных данных пользователя в сам алгоритм машинного обучения, поскольку действующее законодательство применяет понятие «алгоритм» преимущественно по отношению к технологии искусственного интеллекта в целом. В частности, этот термин используется для обозначения алгоритма принятия решений в такой информационной системе [Говорова, 2024. С. 56].

Подобное понимание термина «алгоритм» является избыточно общим, так как работа искусственного интеллекта, а также нейронных сетей, основанных на технологиях машинного обучения, уже по своему содержанию, чем алгоритм принятия решений. В контексте функционирования технологий машинного обучения алгоритмы предполагают наличие определенной информационной системы, представленной машинно-исполняемыми программами, которые написаны с использованием языков программирования. Вне контекста работа системы искусственного интеллекта оказываются простые алгоритмы, упорядочивающие последовательность символьных рядов или осуществляющих простые вычислительные операции. Алгоритмы шифрования, используемые в различных областях криптографических технологий и кибербезопасности, также не тождественны алгоритмам машинного обучения [Минбалеев, Филоненкова, 2020. С. 92].

Для отдельных видов алгоритмов информация в виде массива персональных данных может составлять часть элемента программного кода, внутри которого конфиденциальная информация может находиться в зашифрованном виде и быть недоступной для субъекта персональных данных. Классическим примером здесь могут служить технологии искусственного интеллекта, применяемые для таргетирования рекламы в Интернете, когда предлагаемые пользователю продукты подбираются на основе ранее заявленных им поисковых предпочтений. Персональные данные, такие как история просмотров, геолокация и демографическая информация, используются для создания профилей пользователей, что позволяет рекламодателям более точно нацеливать свои объявления. Нейронные сети способны анализировать огромные объемы данных, выявляя скрытые связи и тренды, которые не всегда заметны при традиционных методах анализа информации, так как при помощи алгоритмов глубокого обучения нейронные сети могут не только обрабатывать текущие персональные данные, но и предсказывать будущие интересы пользователей [Матюк, 2020. С. 129].

Иными словами, алгоритмизованная природа технологий машинного обучения требует наличия определенных информационных предпосылок, частью

Цифровая эпоха

которых может выступать конфиденциальная информация о личности пользователя. Использование этой информации нейронной сетью в определенном смысле является вопросом, подвешенным в воздухе, поскольку юридическая квалификация этой обработки оказывается невозможной в силу отсутствия четких положений закона. Однако потенциально это можно рассматривать как нарушение прав личности на защиту ее персональных данных. Например, если человек начинает активно исследовать определенные продукты в Интернете, нейронная сеть может моментально скорректировать показываемую рекламу, предлагая ему актуальные товары или услуги, основанные на его предпочтениях и предыдущем взаимодействии с контентом [Харитонов, Савина, 2020. С. 525].

Развитие блокчейн-технологии

Одной из наиболее перспективных технологий новой экономики является технология распределенных реестров данных, также известная как «блокчейн». С момента активного внедрения технологии децентрализованного хранения информации в виде непрерывной последовательной цепочки блоков (технология блокчейн), устранившей возможность незаметного изменения информации в распределенной (полностью реплицированной) базе данных, были сформированы необходимые условия для генерации новых форм оборота цифровых активов. Типичной чертой классических баз данных (баз хранения и переработки информации) является возможность незаметного внесения изменений в состав хранимой информации, что требовало привлечения значительных технологических ресурсов для защиты данной информации. Технология полностью реплицированного хранения информации решила данную проблему за счет децентрализованного распределения информации по отдельным блокам, обладающим качеством связанности. Отныне внесение изменений в отдельный блок информации порождало необратимые изменения в других блоках информации, что в условиях децентрализованного хранения делало невозможным незаметное осуществление каких-либо процедур преобразования хранимой информации [Талапина, 2020. С. 29].

Блокчейн обеспечивает новую парадигму безопасности хранения данных, основанную на принципе децентрализации. Ее основной особенностью является прозрачность, так как все данные на блокчейне являются общедоступными, они не могут быть произвольно изменены и легко доступны для проверки. Также особенностью этой технологии является неизменяемость, так как изменение записей в блокчейне является чрезмерно сложным и требует консенсуса, предоставляемого в соответствии с протоколом (например, большинством пользователей блокчейна). Таким образом, целостность записей обеспечивается внутренними

ми свойствами базового кода, а не идентификаторами системных операторов [Добробаба, 2023. С. 37].

Необходимо обозначить важное различие решений на основе технологии блокчейн в публичных (без разрешений) и частных (требующих разрешений) блокчейнах. Публичные блокчейны предоставляют доступ для чтения и возможность создавать транзакции всем пользователям блокчейна. Пользователи могут передавать стоимость без выраженного согласия оператора платформы блокчейн. Основным свойством этих блокчейнов является устойчивость к цензуре, то есть любая действительная транзакция, транслируемая по сети блокчейнов без разрешений, будет включена в блокчейн. Эти различные технологические архитектуры могут иметь радикально разные последствия с точки зрения пользователей и способов использования системы, а также восприимчивости к регулированию и экономической эффективности практик, которым они способствуют [Талапина, 2022. С. 67].

Технология блокчейн сама по себе не обязательно влечет за собой децентрализацию, невмешательство или устранение доверенных посредников. В некоторых областях полное устранение посредников может быть непрактичным, возможным или даже желательным. Это ярко видно в области онлайн-музыки, где многие блокчейн-платформы обещают отсутствие посредников в отношениях между исполнителем и аудиторией.

Взрывное развитие технологии блокчейн привело к появлению ряда блокчейн-приложений в области авторского права, главным образом в секторе онлайн-музыки. Разработка рыночных приложений сопровождалась ростом числа ученых, которые исследуют последствия блокчейна с точки зрения информационного права и технологий, уделяя особое внимание регулированию, интеллектуальным контрактам и появляющемуся направлению исследований в области конфиденциальности и защиты данных [Наумов, 2020. С. 6].

Средний пользователь компьютера сегодня может легко предпринять копирование такого рода и в таком объеме, для которого всего несколько лет назад потребовались бы значительные инвестиции и, возможно, преступный умысел. Также нет технологических ограничений на количество людей, которые могут одновременно получать доступ к таким цифровым объектам буквально из любой точки планеты, где есть подключение к Интернету. Кроме того, современные интернет-технологии позволяют отправлять информационные продукты по всему миру дешево и практически мгновенно. В отличие от традиционных баз данных, которые подвержены рискам утечки информации и несанкционированного доступа, блокчейн обеспечивает высокий уровень защиты благодаря шифрованию и распределению данных среди множества узлов сети. Это означает, что персональные данные пользователей могут храниться исключительно в зашифрованном

виде, а доступ к ним будет осуществляться только при соблюдении строгих условий и с согласия владельцев данных [Мамитова, 2022. С. 28].

В некоторой степени блокчейн можно рассматривать как базу данных с проверенными общедоступными временными метками. Это создает возможность для любого человека публично и неизменно заявить, что определенное событие произошло в определенное время. Таким образом, блокчейн может быть очень полезен для определения презумпции авторства и разрешения споров относительно приоритета в этой сфере. Этот потенциал блокчейна в сфере интеллектуальной собственности уже признан в специализированной литературе. Люди могут использовать веб-сервис для хэширования (функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определенным алгоритмом) таких вещей, как произведения искусства или программное обеспечение, чтобы доказать авторство работ [Смаженков, 2020. С. 578].

С момента активного технологического внедрения блокчейна как передового средства регулирования защиты информации перед множеством государств мира встал вопрос о создании нормативно-правовой базы, регулирующей отношения, связанные с применением данной технологии. Новые типы общественных отношений объективно появляются в связи с глобальным научно-техническим развитием. Информационные технологии проникают во все сферы общественных отношений, трансформируя процессы и процедуры, что обуславливает необходимость гармонизации правового регулирования, формирования цифрового права в целом. Одним из наиболее принципиальных преимуществ использования блокчейна для работы с персональными данными является прозрачность и возможность отслеживания операций. Каждое изменение информации фиксируется в блоке, что создает неизменяемую историю доступа и модификаций данных, что позволяет пользователям отслеживать, кто, когда и как использовал их персональные данные [Марданова, 2024. С. 76].

В период с 2015 по 2019 год в России сформировалась развитая техническая система, предполагающая активное использование технологии блокчейн. Это произошло в банковском секторе, коммерческих компаниях, неправительственных организациях и ассоциациях, которые проводят отдельные исследования и разрабатывают технологии, связанные с использованием технологии блокчейн.

Применение технологий машинного обучения в сфере медицины

Министерство здравоохранения Российской Федерации также объявило о планах перевести электронные записи пациентов в российских медицинских уч-

реждениях в единую справочную систему на основе блокчейна. Граждане смогут самостоятельно выбирать, с кем они будут делиться личной информацией. Нет сомнений в том, что использование новейших технологий открывает большие возможности как для государств и общества в целом, так и для отдельного человека. Несмотря на наличие нескольких перспективных блокчейн-проектов, уровень внедрения этой технологии в России находится на зачаточном уровне. Однако сама по себе обработка этой конфиденциальной информации еще не исчерпывает круг проблем в правовом регулировании защиты персональных данных при работе с технологиями машинного обучения.

Нейронные сети, как известно, могут создавать новые массивы информации на базе уже предоставленных ей сведений о пользователе. Особенностью функционирования технологий машинного обучения является их способность к разработке новых алгоритмических моделей, способных предсказывать поведение пользователя в будущем на основе уже предоставленной ранее информации. Частично, хотя и не в полном объеме, прогностическая функция нейронных сетей может посягать на более значимые для пользователя сведения, которые можно отнести к категории персональных данных, круг которых устанавливается положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных). При этом на сегодняшний день не существует интегрированного источника правового регулирования блокчейна, который пользовался бы авторитетом среди всех участников процесса оборота персональных данных, удовлетворял требованиям понимания блокчейна для государственного регулирования [Сарпеков, 2020. С. 16].

Для области оказания медицинских услуг, в рамках которой критическое значение имеют биометрические данные человека, особенностью режима оборота персональных данных является внутренняя дифференциация сведений, входящих в объем этого понятия. Так, использование технологий машинного обучения в сфере медицины должно опираться на твердое понимание критериев, используемых для отграничения персональных сведений, входящих в состав биометрических данных, от иных типов персональных данных. Обращение в учреждение здравоохранения сопровождается на первоначальном этапе обработкой базовой информации о личности человека, которая доступна также и иным органам государства. И лишь по мере оказания медицинских услуг объем персональных данных пополняется сведениями о здоровье человека, которые в своей совокупности и составляют объем понятия биометрических данных. На сегодняшний день в законодательстве Российской Федерации отсутствуют четкие основания для отграничения биометриче-

Цифровая эпоха

ских данных от иных типов сведений, позволяющих идентифицировать личность человека.

В частности, ст. 11 Закона о персональных данных использует легальную дефиницию рассматриваемого понятия, раскрывая его через общую категорию «физические и биологические особенности человека». Не вполне проясненным остается вопрос о том, поглощает ли собой признак «физические особенности» физиологические признаки личности человека или относится только к сфере его внешнего, физического облика (рост, вес, цвет глаз и проч.).

Вызывает сомнения совмещение в этой дефиниции физиологии и биологии, поскольку физиология выступает в качестве составного раздела биологии как науки о живых существах, что является примером избыточного повторения. С другой стороны, сужение понятия биометрических данных только до уровня физических особенностей человека исключает иные характеристики личности, которые могут быть отнесены к биометрическим данным. Так, одним из перспективных направлений развития современных биометрических технологий является идентификация личности человека по его походке, а также по иным проявлениям его поведения (например, жестам). Между тем научной дисциплиной, которая изучает поведенческие характеристики человека, является этология. Именно поэтому в попытках сконструировать более подходящую дефиницию биометрических данных встречаются формулировки, которые указывают на физические и поведенческие особенности человека, а не на его биологические признаки. В результате

формируется ситуация правовой неопределенности, поскольку оператор персональных данных может испытывать затруднения с отнесением той или иной информации к разряду биометрических данных.

В результате представляется необходимым расширить легальную дефиницию понятия биометрических данных в Законе о персональных данных, изменив содержание части 1 статьи 11 этого нормативно-правового акта и изложив его в следующем виде: «Сведения, характеризующие физиологические, физические и поведенческие признаки человека, позволяющие идентифицировать его личность, которые используются оператором при наличии согласия со стороны субъекта персональных данных, выраженного в письменной форме, за исключением случаев, предусмотренных частью 2 настоящей статьи».

Заключение

Рассмотренные проблемы правового обеспечения защиты персональных данных свидетельствуют о насущной необходимости совершенствования законодательной модели для получения информированного согласия пользователя на обработку персональных данных. В дальнейшем развитии нуждается понятийный аппарат законодательства о защите персональных данных, который должен расширяться по мере усложнения общественных отношений в сфере оборота персональных данных. Активное внедрение новых технологий, связанных с обработкой биометрических данных, должно сопровождаться усовершенствованием критериев дифференциации видов персональных данных.

Литература

- Афанасьева Е.Н. Искусственный интеллект и «большие данные» в здравоохранении: области применения и гражданско-правовое регулирование. *Юридическая наука и практика*. 2020. Т. 16. № 3. С. 40–49. <https://doi.org/10.25205/2542-0410-2020-16-3-40-49>. EDN: PWNKTX
- Аюшеева И.З. Большие данные: проблемы определения гражданско-правового режима. *Lex Russica*. 2023. Т. 76. № 10 (203). С. 125–134. <https://doi.org/10.17803/1729-5920.2023.203.10.125-134>
- Говорова Д.П. Уголовно-правовая охрана персональных данных в условиях цифровизации. *Вестник Северо-Восточного федерального университета имени М.К. Аммосова. Серия: История. Политология. Право*. 2024. № 1 (33). С. 55–59. <https://doi.org/10.25587/2587-5612-2024-1-55-59>
- Добробаба М.Б. Правовое обеспечение защиты персональных данных при использовании технологий искусственного интеллекта. *Информационное право*. 2023. № 3 (77). С. 35–39. <https://doi.org/10.55291/1999-480X-2023-3-35-39>. EDN: MVGNWD
- Литвин И.И. Особенности сбора, обработки и защиты персональных данных искусственным интеллектом. *Вестник Уральского юридического института МВД России*. 2021. № 4 (32). С. 112–118.
- Макаренко Е.А. Решение вопросов этики при внедрении систем с искусственным интеллектом. *Экономика и управление: проблемы, решения*. 2022. Т. 3. № 8 (128). С. 77–82. <https://doi.org/10.36871/ekur.p.r.2022.08.03.009>
- Мамитова Н.В. Цифровая экспертиза в системе оптимизации правового регулирования в Российской Федерации. *Юридическая техника*. 2022. № 16. С. 26–29. EDN: AZVCGE
- Марданова Г.А. Вопросы правового регулирования обработки персональных данных. *Право и экономика*. 2024. № 3 (433). С. 70–76.
- Матюк Ю.С. Правовые и социальные аспекты применения искусственного интеллекта в условиях пандемии. *Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса*. 2020. Т. 12. № 4. С. 129–136. <https://doi.org/10.24866/VVSU/2073-3984/2020-4/129-136>. EDN: EOTKAD
- Минбалева А.В., Сторожакова Е.Э. Проблемы правовой охраны персональных данных в процессе использования нейронных сетей. *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2023. № 2 (102). С. 71–79. <https://doi.org/10.17803/2311-5998.2023.102.2.071-079>. EDN: HHWWAO
- Минбалева А.В., Филоненкова В.А. Проблемы защиты персональных данных и цифрового профиля человека в сети интернет в условиях пандемии. *Вестник Южно-Уральского государственного университета. Серия: Право*. 2020. Т. 20. № 3. С. 89–94. <https://doi.org/10.14529/law200313>
- Наумов В.Б. Теоретические информационно-правовые вопросы идентификации в цифровой сфере. *Информационное право*. 2020. № 4. С. 4–8. EDN: QLHPTQ
- Новикова Ю.А. Категории персональных данных работников. *Вопросы трудового права*. 2024. № 1. С. 22–29. <https://doi.org/10.33920/pol-2-2401-03>. EDN: IAPYWW
- Сарпеков Р.К. Цифровизация правового пространства. *Вестник Института законодательства и правовой информации Республики Казахстан*. 2020. № 3 (61). С. 12–24.

Свиридова Е.А. Открытые и персональные данные в системах искусственного интеллекта: правовые аспекты. *Проблемы экономики и юридической практики*. 2021. Т. 17. № 6. С. 61–68. EDN: XOKZIK

Смаженков Н.С. Нормативно-правовое регулирование защиты персональных данных в условиях использования цифровых технологий. *Вопросы российской юстиции*. 2020. № 7. С. 576–583. EDN: JHAVGN

Талапина Э.В. Автоматизированное принятие решений в государственном управлении: теоретический разбор возможностей. *Журнал российского права*. 2022. Т. 26. № 11. С. 60–73. <https://doi.org/10.12737/jrl.2022.117>. EDN: HFFCKT

Талапина Э.В. Алгоритмы и искусственный интеллект сквозь призму прав человека. *Журнал российского права*. 2020. № 10. С. 25–39. <https://doi.org/10.12737/jrl.2020.118>

Харитонова Ю.С., Савина В.С. Технология искусственного интеллекта и право: вызовы современности. *Вестник Пермского университета. Юридические науки*. 2020. № 49. С. 524–549. <https://doi.org/10.17072/1995-4190-2020-49-524-549>. EDN: YDGFTN

References

- Afanas'yeva E.N. Artificial Intelligence and «Big Data» in healthcare: applications and legal regulation. *Yuridicheskaya nauka i praktika*. 2020. Vol. 16. No. 3. P. 40–49. <https://doi.org/10.25205/2542-0410-2020-16-3-40-49>. EDN: PWNKTX. In Russian
- Ayusheeva I.Z. Big data: problems of defining the civil-law regime. *Lex Russica*. 2023. Vol. 76. No. 10 (203). P. 125–134. <https://doi.org/10.17803/1729-5920.2023.203.10.125-134>. In Russian
- Dobrobaba M.B. Legal protection of personal data when using artificial intelligence technologies. *Informatsionnoye pravo*. 2023. No. 3 (77). P. 35–39. <https://doi.org/10.55291/1999-480X-2023-3-35-39>. EDN: MVGNWD. In Russian
- Govorova D.P. Criminal law protection of personal data in the context of digitalization. *Vestnik Severo-Vostochnogo federal'nogo universiteta imeni M.K. Ammosova. Seriya: Istoriya. Politologiya. Pravo*. 2024. No. 1 (33). P. 55–59. <https://doi.org/10.25587/2587-5612-2024-1-55-59>. In Russian
- Kharitonova Yu.S., Savina V.S. Artificial Intelligence technology and law: challenges of our time. *Vestnik Permskogo universiteta. Yuridicheskiye nauki*. 2020. No. 49. P. 524–549. <https://doi.org/10.17072/1995-4190-2020-49-524-549>. EDN: YDGFTN. In Russian
- Litvin I.I. Features of collecting, processing, and protecting personal data by artificial intelligence. *Vestnik Uralskogo yuridicheskogo instituta MVD Rossii*. 2021. No. 4 (32). P. 112–118. In Russian
- Makarenko E.A. Addressing ethical issues in the implementation of systems with Artificial Intelligence. *Ekonomika i upravleniye: problemy, resheniya*. 2022. Vol. 3. No. 8 (128). P. 77–82. <https://doi.org/10.36871/ekup.p.r.2022.08.03.009>. In Russian
- Mamitova N.V. Digital expertise in the system of optimization of legal regulation in the Russian Federation. *Yuridicheskaya tekhnika*. 2022. No. 16. P. 26–29. EDN: AZVCGE. In Russian
- Mardanov G.A. Issues of legal regulation of personal data processing. *Pravo i ekonomika*. 2024. No. 3 (433). P. 70–76. In Russian
- Matyuk Yu.S. Legal and social aspects of the use of artificial intelligence during a pandemic. *Territoriya novykh vozmozhnostey. Vestnik Vladivostokskogo gosudarstvennogo universiteta ekonomiki i servisa*. 2020. Vol. 12. No. 4. P. 129–136. <https://doi.org/10.24866/VVSU/2073-3984/2020-4/129-136>. EDN: EOTKAD. In Russian
- Minbaleev A.V., Filonenkova V.A. Problems of personal data protection and a digital profile of a person on the internet in the context of a pandemic. *Vestnik Yuzhno-Uralskogo gosudarstvennogo universiteta. Seriya: Pravo*. 2020. Vol. 20. No. 3. P. 89–94. <https://doi.org/10.14529/law200313>. In Russian
- Minbaleev A.V., Storozhakova E.E. Problems of legal protection of personal data in the process of using neural networks. *Vestnik Universiteta imeni O.Ye. Kutafina (MGYU)*. 2023. No. 2 (102). P. 71–79. <https://doi.org/10.17803/2311-5998.2023.102.2.071-079>. EDN: HHWWAO. In Russian
- Naumov V.B. Theoretical information and legal issues of identification in the digital sphere. *Informatsionnoye pravo*. 2020. No. 4. P. 4–8. EDN: QLHPTQ. In Russian
- Novikova Yu.A. Categories of personal data of employees. *Voprosy trudovogo prava*. 2024. No. 1. P. 22–29. <https://doi.org/10.33920/pol-2-2401-03>. EDN: IAPYWW. In Russian
- Sarpekov R.K. Digitalization of the legal space. *Vestnik Instituta zakonodatelstva i pravovoy informatsii Respubliki Kazakhstan*. 2020. No. 3 (61). P. 12–24. In Russian
- Smazhenkov N.S. Legal regulation of personal data protection in the context of using digital technologies. *Voprosy rossiyskoy yustitsii*. 2020. No. 7. P. 576–583. EDN: JHAVGN. In Russian
- Sviridova E.A. Open and personal data in artificial intelligence systems: legal aspects. *Problemy ekonomiki i yuridicheskoy praktiki*. 2021. Vol. 17. No. 6. P. 61–68. EDN: XOKZIK. In Russian
- Talapina E.V. Algorithms and artificial intelligence through the prism of human rights. *Zhurnal rossiyskogo prava*. 2020. No. 10. P. 25–39. <https://doi.org/10.12737/jrl.2020.118>. In Russian
- Talapina E.V. Automated decision-making in public administration: a theoretical analysis of the possibilities. *Zhurnal rossiyskogo prava*. 2022. Vol. 26. No. 11. P. 60–73. <https://doi.org/10.12737/jrl.2022.117>. EDN: HFFCKT. In Russian

ИНФОРМАЦИЯ ОБ АВТОРЕ:

Сергей Владимирович Дейко, заместитель директора по экономическим и финансовым вопросам Научно-исследовательский институт «Восход» (Российская Федерация, 119607, Москва, ул. Удальцова, 85). E-mail: nauka-msk@yandex.ru

Для цитирования: Дейко С.В. Актуальные аспекты защиты персональных данных в условиях внедрения технологий машинного обучения. *Государственная служба*. 2025. № 3. С. 67–73.

INFORMATION ABOUT THE AUTHOR:

Sergey V. Deiko, Deputy Director for Economic and Financial Issues Scientific Research Institute Voskhod (85, Udaltsova St., Moscow, 119607, Russian Federation). E-mail: nauka-msk@yandex.ru

For citation: Deiko S.V. Current aspects of personal data protection in the context of implementing machine learning technologies. *Gosudarstvennaya sluzhba*. 2025. No. 3. P. 67–73.