УДК 340-13
DOI: https://doi.org/10.17308/law/1995-5502/2024/4/44-51

К ВОПРОСУ О ПРАВОВОМ РЕЖИМЕ ОБЕЗЛИЧЕННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Н. А. Жирнова, О. Л. Солдаткина
Национальный исследовательский университет «Высшая школа экономики» (Москва)

ON THE ISSUE OF THE LEGAL REGIME OF DEPERSONALIZED PERSONAL DATA

N. A. Zhirnova, O. L. Soldatkina
National Recearch University «Higher School of Economics» (Moscow)

Аннотация: статья посвящена актуальной в свете тенденций по созданию «регуляторного рая» для разработчиков систем искусственного интеллекта проблеме установления эффективного правового режима для обезличенных персональных данных. В данном сегменте законодательства сегодня происходят изменения, не все из которых можно назвать удачными. Вместе с этим от решения указанной проблемы напрямую зависит успех развития перспективной отрасли по созданию искусственного интеллекта. В ходе исследования авторы проводят разработку каждого из элементов правового режима обезличенных персональных данных, сделав акцент на необходимость принятия мер по охране информации. Кроме того, в статье исследуются подходы к решению обозначенной проблемы в других странах и даются некоторые рекомендации по изменению законодательной и правоприменительной практики в сфере оборота обезличенных персональных данных.
Ключевые слова: правовой режим, правовое регулирование персональных данных, персональные данные, обезличенные персональные данные, анонимизированные данные.

Abstract: the article is devoted to the problem of establishing an effective legal regime for depersonalized personal data, which is relevant in light of the trends to create a «regulatory paradise» for developers of artificial intelligence systems. Changes are taking place in this segment of legislation today, not all of which can be called successful. At the same time, the success of the development of a promising industry for the creation of artificial intelligence directly depends on how the problem is solved. In the course of the study, the authors develop each of the elements of the legal regime, focusing on taking measures to protect information. In addition, approaches to solving the problem in other countries are studied and some recommendations are given for changing the attitude to the concept of depersonalized personal data.
Key words: legal regime, legal regulation of personal data, personal data, depersonalized personal data, anonymized data.

Сегодня одной из актуальнейших проблем является необходимость установления «правил игры» для общественных отношений, складывающихся с участием искусственного интеллекта. Однако в России, да и в большинстве стран мира, в настоящий момент ситуацию, сложившуюся в сфере нормативно-правового регулирования вышеуказанного феномена, нельзя признать адекватной требованиям и вызовам цифровизации. При этом российские законодатели заявляют о полной поддержке разработчиков искусственного интеллекта и создании для них в России «регуляторного рая»[1], без уточнения, что для этого нужно.

[1] См., например: Чернышенко : Экономический эффект от внедрения ИИ составил более триллиона рублей // Парламентская газета. 2024. 13 мая. URL: https://www.pnp.ru/politics/chernyshenko-ekonomicheskiy-effekt-ot-vnedreniya-ii-sostavil-bolee-trilliona-rubley.html?ysclid=lztx0ass61360640966 (дата обращения: 14.08.2024).

Еще в 2006 г. вице-президент американской Ассоциации рекламодателей (Association of National Advertisers) Майкл Палмер подтвердил и развил мысль бизнесмена Клайв Хамби о сходстве данных и топлива: «Данные похожи на сырую нефть. Оно полезно, но в необработанном виде непригодно для использования»[2]. Эта метафора не теряет своей актуальности и сегодня, хотя у нее есть и критики: эксперты писали и о том, что аналогия между данными и нефтью не работает, что данные могут быть токсичными или даже «мусорными»[3].

Несмотря на красочность и ненаучный стиль приведенных высказываний, в них есть определенный смысл: искусственному интеллекту требуются данные для обучения – и чем объемнее и качественнее будет выборка, тем лучше будут результаты обучения. В ряде случаях такая необходимость вступает в конфликт с конфиденциальностью отдельных видов информации, например персональных данных. Компромиссом в данной сфере является использование для обучения искусственного интеллекта обезличенных персональных данных. В силу сказанного никакой «регуляторный рай» в сфере искусственного интеллекта невозможен без установления грамотного правового режима обезличенных персональных данных, так как именно они занимают особое место в структуре так называемых «больших данных» (Big Data), являющихся, в свою очередь, критично важными для обучения искусственного интеллекта.

Прежде чем говорить о составляющих правового режима обезличенных персональных данных, следует определиться с нашим подходом к пониманию правового режима.

Анализ научных источников показывает, что, с одной стороны, тема научных режимов достаточно разработана[4], с другой – понятие часто используется как само собой разумеющееся. В целом, термин можно считать устоявшимся, а нюансы его определения зависят от того, в рамках какого направления правоведения он рассматривается. Так, Г. С. Беляева только среди общетеоретических подходов к дефиниции анализируемого юридического феномена выделяет три основных, а также некоторый интеграционный[5]. Поскольку рассматриваемый вопрос относится к информационному праву, близкому по природе к административному праву, в рамках нашего исследования стоит ориентироваться на мнение представителей указанных разделов правоведения.

Д. Н. Бахрах писал, что «правовой режим – это официально установленный особый порядок правового регулирования, отражающий совокупность юридических и организационных средств, используемых для закрепления социально-правового состояния объектов воздействия и направленный на обеспечение их устойчивого функционирования»[6] (что перекликается в целом с общетеоретическим инструментальным подходом).

Выделим дефиницию Н. Н. Ковалевой для более узкого понятия «правовой режим информационных ресурсов», определяемого как «возможность совершения или несовершения с объектом права определенных действий, влекущих известный юридический результат»[7]. Данный вариант определения правового режима представляет интерес по нескольким причинам. Во-первых, персональные данные по природе являются информационным ресурсом. Во-вторых, у определения в работах Н. Н. Ковалевой есть развитие – отмечаются составляющие правового режима информационных ресурсов:

1) порядок документирования информации;

2) положения о доступе к информационным ресурсам в зависимости от их категорий;

3) принятие мер по охране информации (способы охраны и порядок их применения)[8].

Таким образом, если констатировать наличие всех трех составляющих, то можно с уверенностью утверждать, что правовой режим того или иного вида информационного ресурса установлен. В целом, поскольку на правовом поле основной единицей информации являет-

[2] *Palmer M.* Data is the New Oil // Ana.blogs.com. 2006. November, 3. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html (дата обращения: 14.08.2024).

[3] См.: *Jason James.* Data as the new oil : the danger behind the mantra. URL: https://enterprisersproject.com/article/2019/7/data-science-data-can-be-toxic (дата обращения: 14.08.2024).

[4] Поиск по запросу «правовой режим» (период с 2014 по 2024 г.) только в названиях исследований на платформе e-library дает в результате 6456 публикаций.

[5] См.: *Беляева Г. С.* Правовой режим : понятие и признаки // Вестник Рос. ун-та дружбы народов. Серия: Юридические науки. 2021. Т. 25, № 1. С. 281–293.

[6] *Бахрах Д. Н.* Административное право : учебник. М., 2011. С. 410.

[7] *Ковалева Н. Н.* Информационное право : учеб. пособие. М., 2010. С. 38.

[8] См: Там же.

ся документ, подход Н. Н. Ковалевой можно распространить на любой вид рассматриваемой в юридической науке информации, в том числе и на обезличенные персональные данные, что и поможет разработать их научно обоснованный правовой режим.

Под обезличенными персональными данными в российском законодательстве понимаются персональные данные, подвергнутые процедуре обезличивания, а под обезличиванием – «действие, в результате которого становится невозможным определить принадлежность персональных данных конкретному субъекту персональных данных»[9].

Документирование информации в самом общем виде можно определить как процесс создания документа, т. е. «придание» информации свойств документа[10], по сути, фиксирование (запись) информации на материальный носитель, присвоение необходимых реквизитов и т. д. Правила документирования информации, являющейся предметом исследования, зафиксированы в целом ряде документов: Приказе Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных»[11], Приказе МВД России от 14 ноября 2017 г. № 852 «Об утверждении Правил работы с обезличенными данными в случае обезличивания персональных данных в Министерстве внутренних дел Российской Федерации»[12] и т. п., а также в локальных нормативных актах конкретной организации, посвященных обработке персональных данных вообще и обезличенных в частности (Парольная политика, Правила резервного копирования, Правила доступа в помещения и т. д.).

Следующая составляющая правового режима информационных ресурсов – выработка правил доступа к ним[13]. Представляется, что в случае с обезличенными персональными данными имеет значение множество факторов, в том числе способы их сбора и анализа, а также – самое главное – методы и приемы, позволяющие на их основе построить эффективные технологические решения. И «особо тонкое» место здесь лежит именно в сфере сбора данных. Данные собираются разными способами, в том числе в сети Интернет. И неправильный правовой режим обезличенных данных может стать «серьезным препятствием на пути развития искусственного интеллекта»[14].

Наконец, третья составляющая правового режима информационных ресурсов – принятие мер по охране информации, в нашем случае – обезличенных персональных данных.

Несмотря на то что данные носят обезличенный характер, это не меняет их правовую природу, а именно – принадлежность к конфиденциальной информации, т. е. такой информации, доступ других лиц к которой ограничен в соответствии с действующим законодательством или по воле обладателя такой информации (последнее актуально для коммерческой тайны, например). И данное обстоятельство, по мнению ряда экспертов[15], серьезно препятствует развитию систем искусственного интеллекта, так как обезличенные персональные данные составляют весьма весомую часть в составе «больших данных».

---

[9] О персональных данных : федер. закон от 27 июля 2006 г. № 152-ФЗ (в ред. от 08.08.2024) // Собр. законодательства Рос. Федерации. 2006. № 31, ч. 1. Ст. 3451 (далее – Закон № 152-Ф).

[10] Документ – материальный носитель с зафиксированной на нем в любой форме информацией в виде текста, звукозаписи, изображения и (или) их сочетания, который имеет реквизиты, позволяющие его идентифицировать, и предназначен для передачи во времени и в пространстве в целях общественного использования и хранения (ст. 1 Федерального закона от 29 декабря 1994 г. № 77-ФЗ «Об обязательном экземпляре документов» // Собр. законодательства Рос. Федерации. 1995. № 1. Ст. 1).

[11] Об утверждении требований и методов по обезличиванию персональных данных : приказ Роскомнадзора РФ от 5 сентября 2013 г. № 996 // Рос. газета. 2013. 18 сент.

[12] Об утверждении Правил работы с обезличенными данными в случае обезличивания персональных данных в Министерстве внутренних дел Российской Федерации : приказ МВД России от 14 ноября 2017 г. № 852 // Официальный интернет-портал правовой информации (http://www.pravo.gov.ru). 2018. 15 янв.

[13] В соответствии с нормами ч. 1 ст. 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (Собр. законодательства Рос. Федерации. 2006. № 31, ч. 1, ст. 3448) доступ к информации – это возможность получения информации и ее использования.

[14] *Ковалева Н. Н., Жирнова Н. А.* Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта // Журнал рос. права. 2024. Т. 28, № 7. С. 109–121.

[15] См., например: *Гаврилюк А.* Бизнес просит депутатов не усложнять работу с обезличенными данными // Forbes. URL: https://www.forbes.ru/tekhnologii/505257-biznes-prosit-deputatov-ne-usloznat-rabotu-s-obezlicennymi-dannymi?ysclid=lzwr51t2ac604118895 (дата обращения: 15.08.2024).

Обращаясь к способам защиты персональных данных, содержащимся в российском (и не только) законодательстве, следует отметить, что центральное место здесь занимает такое условие их обработки, как наличие согласия на то субъекта персональных данных (ч. 1 ст. 6 Закона № 152-ФЗ), при этом закон допускает обработку персональных данных без согласия субъекта в статистических или иных исследовательских целях, при условии обязательного обезличивания этих данных в соответствии с п. 9 ч. 1 ст. 6 Закона № 152-ФЗ.

В силу прямого указания закона такая обработка не должна использоваться в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации (ст. 15 Закона № 152-ФЗ). Подчеркнем также, что это основание не распространяется на специальные категории персональных данных.

Основной вопрос состоит в том, что многие исследования и разработки ведут коммерческие организации, что несомненно хорошо понимают и законодатели. Государство делает шаги навстречу бизнесу, но важно, чтобы эти шаги были максимально эффективными при соблюдении баланса между необходимостью технологического развития и защитой прав граждан – речь идет об изменениях в законопроекте «О персональных данных», уточняющих порядок обработки персональных данных. Сам законопроект был внесен в Госдуму еще в 2020 г. и принят в первом чтении в 2021 г. Как следует из текста пояснительной записки, главный аспект – создание единого государственного хранилища персональных данных, которое должны быть реализовано в формате Государственной информационной системы.

В дальнейшем законопроект был существенно переработан и в результате работы был принят Федеральный закон от 30 июля 2024 г. № 233-ФЗ «О внесении изменений в Федеральный закон “О персональных данных” и Федеральный закон “О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона ‘‘О персональных данных”»[16] (далее – Закон № 233-ФЗ).

Новый закон, по задумке его авторов, призван обеспечить доступ бизнес-структур (прежде всего, разработчиков искусственного интеллекта) к данным россиян «для развития технологий» и при этом призван исключить возможность установления личности человека по этой информации. В соответствии с положениями данного нормативного акта необходимые массивы (наборы) данных будут формироваться для конкретных случаев, определить которые еще предстоит Правительству РФ. Работа с массивами данных будет осуществляться в специальной государственной информационной системе (далее – ГИС), имеющей закрытый контур.

Спроектированное регулирование критиковалось представителями бизнес-сообщества еще на этапе законопроекта: акцент делался на то, что реализация закона потребует значительных государственных затрат, а получившаяся ГИС будет уязвима в случае диверсий. Кроме того, эксперты высказывают опасения относительно рисков монополизации государством работы с данными, отсутствия обмена обезличенными персональными данными и датасетами на их основе и т. д.

Закон вступает в силу 1 сентября 2025 г., нельзя исключить и возможность внесение изменений. Более того, в законе речь идет об экспериментальном правовом режиме, поэтому интересно рассмотреть разные варианты данного регулирования.

Однако думается, что корень проблемы лежит, прежде всего, в области подхода к тому, что именно следует понимать под обезличенными данными – от этого будет напрямую зависеть и третья составляющая правового режима.

Представляется, что приведенная ранее имеющаяся в отечественном законодательстве конструкция относительно процесса обезличивания не является удачной, так как оставляет любые данные, полученные таким образом, персональными. Такой вариант не упрощает сбор информации для обучения искусственного интеллекта,

[16] О внесении изменений в Федеральный закон «О персональных данных» и Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона ‘‘О персональных данных» : федер. закон от 30 июля 2024 г. № 233-ФЗ // Собр. законодательства Рос. Федерации. 2024. № 33, ч. 1. Ст. 4929.

оставляя ситуацию по сути такой же, как и была до принятия Закона № 233-ФЗ. Рассмотрим практику разных стран по решению данного вопроса.

США

В США отсутствует единый национальный закон о персональных данных, что в целом характерно для системы общего права: сфера защиты персональных данных здесь регулируется сложной совокупностью законов как федерального уровня, так и уровня отдельных штатов. Подходы к тому, что именно считать обезличенными данными, также разные.

Медицинские данные

Закон о переносимости и подотчетности медицинского страхования 1996 г. (Health Insurance Portability and Accountability Act of 1996)[17] определяет понятие de-identified data (неидентифицируемые данные) следующим образом: «Информация о состоянии здоровья, которая не идентифицирует личность и в отношении которой нет разумных оснований полагать, что она может быть использована для идентификации личности». При этом деидентификация может быть обратимой, если субъект, деидентифицирующий данные, создает ключ, сопоставляющий замаскированные значения с прямыми идентификаторами.

Образование

Федеральный закон о праве на неприкосновенность частной жизни в сфере образования (Family Educational Rights and Privacy Act, FERPA)[18] определяет, что данные деидентифицируются, если для любого набора квазиидентификаторов, которые есть у сущности в наборе данных, в наборе данных есть по крайней мере четыре других лица с тем же набором квазиидентификаторов. Таким образом, если набор данных содержит ваш пол, дату рождения и почтовый индекс (и никаких других квазиидентификаторов), то в наборе данных должно быть по крайней мере четыре других записи с вашими такими же характеристиками.

Законодательство штатов Калифорния – CCPA/CPRA и CalOPPA

Закон штата Калифорния о конфиденциальности потребителей (California Consumer Privacy Act, CCPA)[19] был принят в 2018 г., но уже в 2020 г. был принят Закон Калифорнии о правах на конфиденциальность 2020 г. (California Privacy Rights Act of 2020, CPRA)[20], существенно расширивший CCPA, предоставив потребителям больший контроль над своими личными данными и создавая Калифорнийское агентство по защите конфиденциальности (CPPA, далее – Агенство). Именно CPRA сделал законодательство Калифорнии о конфиденциальности данных наиболее полным в США.

CCPA определяет «обезличенную информацию» как «данные, которые не могут обоснованно идентифицировать, соотносить, описывать, ассоциировать или быть связаны, прямо или косвенно, с конкретным потребителем» и прямо исключает такую информацию из перечня персональной информации.

CCPA (CPRA) рассматривает информацию, которая не может обоснованно идентифицировать конкретного потребителя, как деидентифицированную информацию. Оговорка заключается в том, что организация должна внедрить бизнес-процессы и технические меры безопасности, которые предотвратят ее повторную идентификацию.

В Колорадо, Коннектикуте, Делавэре, Флориде, Индиане, Айове, Монтане, Нью-Джерси, Орегоне, Теннесси, Техасе, Юте, Вирджинии персональные данные включают информацию, которая связана с идентифицированным или идентифицируемым лицом – резидентом конкретного штата или домохозяйством. Обезличенные данные, ставшие общедоступными персональные данные, персональные данные о лицах, действующих в контексте трудоустройства чаще всего не входят в сферу применения законодательства.

Такое разнообразие в терминологии и средствах обезличивания для российского законодательства не очень подходит в силу своей технологичности.

GDPR

Согласно параграфу 5 ст. 4 Общего регламента по защите персональных данных (General Data Protection Regulation, GDPR) псевдонимизация – это «обработка персональных данных таким об-

[17] Health Insurance Portability and Accountability Act of 1996. URL: https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996 (дата обращения: 14.08.2024).

[18] Family Educational Rights and Privacy Act (20 U.S.C. § 1232g; 34 CFR Part 99). URL: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (дата обращения: 14.08.2024).

[19] California Consumer Privacy Act. URL: https://theccpa.org/ (дата обращения: 18.06.2024).

[20] California Privacy Rights Act of 2020. URL: https://thecpra.org/ (дата обращения: 18.06.2024).

разом, что их больше невозможно отнести к конкретному субъекту данных без использования дополнительной информации, при условии, что такая дополнительная информация хранится отдельно, и в отношении нее приняты технические и организационные меры, предотвращающие ее отнесение идентифицированному или идентифицируемому физическому лицу».

Технически псевдонимизация данных (определение дано в ст. 4(5) GDPR) означает замену любой информации, которая может быть использована для идентификации личности, псевдонимом или, другими словами, значением, которое не позволяет напрямую идентифицировать личность. Но такие данные остаются персональными данными, т.е. использование псевдонимизации не подразумевает отказ от каких-либо иных мер защиты персональных данных. Целями процесса являются снижение рисков для соответствующих субъектов данных и помощь контролерам и процессорам данных в выполнении их обязанности по защите персональных данных.

В отличие от псевдонимизации, которая повышает защиту данных, но по-прежнему оставляет их персональными, анонимизация делает данные анонимными, т. е. не персональными.

В соответствии с преамбулой 26 GDPR, принципы защиты персональных данных не применяются в отношении анонимной информации, а именно информации, которая не относится к идентифицированному или идентифицируемому физическому лицу, а также в отношении персональных данных, предоставленных достаточно анонимно, чтобы субъект данных не мог быть идентифицированным.

GDPR не применяется в отношении обработки анонимной информации, в том числе в статистических или исследовательских целях.

Если попытаться провести аналогию с российским законодательством, то обезличивание персональных данных по своему содержанию соответствует псевдонимизации, а не анонимизации. В связи с этим международный эксперт Сергей Воронкевич (Минск) поясняет, что «анонимизация по GDPR подразумевает невозможность установить личность индивида даже при наличии дополнительных сведений. Например, если вы не можете узнать человека по фотографии, но у вас есть Интернет и доступ к поиску по картинкам Google, то данное изображение представляет собой не анонимную, а псевдонимную информацию»[21]. Как видим, российский концепт «обезличивание» по природе близок к европейской анонимизации.

Несмотря на то что ЕС нельзя назвать страной с самым «дружелюбным» для развития искусственного интеллекта законодательством, но именно GDPR по праву считается одним из самых проработанных актов, посвященных теме персональных данных, в мире. Многие озвученные в GDPR подходы находят отражение в законах других стран. В подтверждении можно привести опыт Китая, традиционно упоминаемого в числе лидеров по развитию цифровых технологий[22]. Закон Китайской Народной Республики о защите личной информации (Personal Information Protection Law of the People's Republic of China, PIPL)[23], принятый на 30-м заседании Постоянного комитета Всекитайского собрания народных представителей 13-го созыва 20 августа 2021 г., содержит аналогичное GDPR разделение анонимизированной информации на 2 категории:

– де-идентификация – обработка персональной информации, которая гарантирует невозможность идентификации конкретного физического лица без использования дополнительной информации (соответствует европейской «псевдонимизации»);

– анонимизация – обработка персональной информации таким образом, чтобы сделать невозможным выделение конкретного физического лица и невозможность восстановления данных.

В российском законодательстве аналог анонимизации же отсутствует, что, учитывая опыт других государств, представляется упущением и должно быть исправлено.

[21] *Садовников Д.* Обезличивание персональных данных в России и в Европе : когда данные перестают быть персональными? // zakon.ru. 2021. 11 мая. URL: https://zakon.ru/blog/2021/11/05/obezlichivanie_personalnyh_dannyh_v_rossii_i_v_evrope_kogda_dannye_perestayut_byt_personalnymi (дата обращения: 18.06.2024).

[22] См., например: Россия вошла в топ-20 стран по развитию цифровых технологий // Роспатент. 2023. 18 янв.

[23] См.: Personal Information Protection Law of the People's Republic of China // Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021. URL: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ (дата обращения: 18.06.2024).

Таким образом, в российском законодательстве (желательно федерального уровня) необходимо ввести разные понятия в зависимости от целей, например, следующим образом.

Обезличенные персональные данные – персональные данные, в отношении которых произведены действия, в результате которых становится невозможным без использования дополнительной информации или программных средств определить принадлежность персональных данных конкретному субъекту персональных данных. Цель – защищать конфиденциальность субъектов данных.

Анонимизированные данные – данные, в отношении которых произведены действия, в результате которых становится абсолютно невозможным определить принадлежность персональных данных конкретному субъекту персональных данных. Цель – вывести часть информации из-под действия закона о персональных данных для обеспечения того самого «регуляторного рая» для компаний, занимающихся развитием искусственного интеллекта.

Библиографический список

Бахрах Д. Н. Административное право России : учебник. 5-е изд., перераб. и доп. М. : Эксмо, 2010. 702 с.

Беляева Г. С. Правовой режим : понятие и признаки // Вестник Рос. ун-та дружбы народов. Серия: Юридические науки. 2021. Т. 25, № 1. С. 281–293.

Ковалева Н. Н. Информационное право : учеб. пособие. М. : Дашков и Ко, 2010. 352 с.

Ковалева Н. Н., Жирнова Н. А. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта // Журнал российского права. 2024. Т. 28, № 7. С. 109–121.

Садовников Д. Обезличивание персональных данных в России и в Европе : когда данные перестают быть персональными? // Zakon.ru. 2021. 11 мая. URL: https://zakon.ru/blog/2021/11/05/obezlichivanie_personalnyh_dannyh_v_rossii_i_v_evrope_kogda_dannye_perestayut_byt_personalnymi

Palmer M. Data is the New Oil // Ana.blogs.com. 2006. November, 3. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Smith M. D., Waldo J. Anonymity, De-Identification, and the Accuracy of Data // Harvardonline. 2023. August, 28. URL: https://www.harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data

References

Bakhrakh D. N. Administrative Law of Russia : textbook. 5th ed., revised. and add. M. : Eksmo, 2010. 702 p.

Belyaeva G. S. Legal regime : concept and features // Bulletin of the Peoples' Friendship University of Russia. Series: Legal Sciences. 2021. Vol. 25, No. 1. P. 281–293.

Kovaleva N. N. Information law : textbook. Moscow : Dashkov i Ko, 2010. 352 p.

Kovaleva N. N., Zhirnova N. A. Problems of ensuring the confidentiality of personal data when using artificial intelligence systems // Journal of Russian Law. 2024. Vol. 28, No. 7. P. 109–121.

Sadovnikov D. Depersonalization of personal data in Russia and Europe : when does data cease to be personal? // Zakon.ru. 2021. May 11. URL: https://zakon.ru/blog/2021/11/05/obezlichivanie_personalnyh_dannyh_v_rossii_i_v_evrope_kogda_dannye_perestayut_byt_personalnymi

Palmer M. Data is the New Oil // Ana.blogs.com. 2006. November, 3. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Smith M. D., Waldo J. Anonymity, De-Identification, and the Accuracy of Data // Harvardonline. 2023. August, 28. URL: https://www.harvardonline.harvard.edu/blog/anonymity-de-identification-accuracy-data

Национальный исследовательский университет «Высшая школа экономики» (Москва)

Жирнова Н. А., кандидат юридических наук, доцент департамента права цифровых технологий и биоправа факультета права

E-mail: natalyazhirnova79@mail.ru

Солдаткина О. Л., кандидат юридических наук, доцент департамента права цифровых технологий и биоправа факультета права

E-mail: buzum@mail.ru

National Recearch University «Higher School of Economics» (Moscow)

Zhirnova N. A., Candidate of Law, Associate Professor of School of Digital Law and Bio-Law of the Law Faculty

E-mail: natalyazhirnova79@mail.ru

Soldatkina O. L., Candidate of Law, Associate Professor of School of Digital Law and Bio-Law of the Law Faculty

E-mail: buzum@mail.ru

Поступила в редакцию: 08.10.2024

Для цитирования:
Жирнова Н. А., Солдаткина О. Л. К вопросу о правовом режиме обезличенных персональных данных // Вестник Воронежского государственного университета. Серия: Право. 2024. № 4 (59). С. 44–51. DOI: https://doi.org/10.17308/law/1995-5502/2024/4/44-51

Received: 08.10.2024

For citation:
Zhirnova N. A., Soldatkina O. L. On the issue of the legal regime of depersonalized personal data // Proceedings of Voronezh State University. Series: Law. 2024. № 4 (59). P. 44–51. DOI: https://doi.org/10.17308/law/1995-5502/2024/4/44-51