DOI: 10.22394/3034-2813-2024-3-96-106 EDN: RYDIZZ

Дата поступления статьи: 17.04.2024
Дата поступления рецензии: 19.05.2024
Дата принятия статьи к публикации: 24.06.2024

Регулирование и защита персональных медицинских данных в эпоху ИИ: международный опыт

Галкина Н. М.[1,*], **Кузнецова Д. В.**[1,**]
[1] Национальный исследовательский университет «Высшая школа экономики» (Москва, Российская Федерация)
[*] e-mail: ngalkina@hse.ru
[**] e-mail: dvkuznetsova@hse.ru

Аннотация
Искусственный интеллект активно захватывает сферу за сферой, в том числе особые успехи и достижения можно видеть в сфере медицины и медицинских технологий. Однако внедрение искусственного интеллекта ставит целый ряд вопросов как практического, так и этического характера. Управление персональными данными становится ключевым вопросом при разработке искусственного интеллекта в медицине, поскольку эффективность таких систем напрямую зависит от доступа к обширным медицинским данным пациентов. Самым удобным решением для их использования является предварительная анонимизация. Однако при анонимизации существует риск повторной идентификации, а также возможна утрата потенциала информативности данных. В рамках настоящей статьи на примере США, ЕС и Сингапура рассматривается опыт в сфере правового регулирования обращения с медицинскими персональными данными при использовании систем искусственного интеллекта в медицине. Каждая из стран пытается найти баланс между защитой конфиденциальности персональных данных и развитием инноваций. На основе проведенного анализа можно сделать вывод, что фокус на развитие искусственного интеллекта требует определенных допущений в области защиты персональных данных, в то время как высокий жесткий стандарт защиты персональных данных может оказывать сдерживающее действие.
Ключевые слова: искусственный интеллект, ИИ, медицинские данные, большие данные, конфиденциальность персональных данных.
Для цитирования: Галкина Н. М., Кузнецова Д. В. Регулирование и защита персональных медицинских данных в эпоху ИИ: международный опыт // Теоретическая и прикладная юриспруденция. 2024. № 3 (21). С. 96–106. DOI: 10.22394/3034-2813-2024-3-96-106. EDN: RYDIZZ

Regulation and protection of personal health data in the AI era: international experience

Galkina N. M.[1,*], **Kuznetsova D. V.**[1,**]
[1] National Research University Higher School of Economics (Moscow, Russian Federation)
[*] e-mail: ngalkina@hse.ru
[*] e-mail: dvkuznetsova@hse.ru

Abstract
Artificial intelligence is actively taking over sphere after sphere and particular successes and achievements can be seen in the medical sector and medical technology. However, the introduction of AI raises a number of practical and ethical issues. One of the main ones is the issue of handling personal

data, as access to a large number of patients' health data plays a key role in the development and use of AI in medicine. The most convenient solution for their use is to anonymise them beforehand. However, with anonymisation, there is a risk of re-identification and the potential for loss of data informativeness may be lost. In the framework of this article the experience in the sphere of legal regulation of personal health data handling when using artificial intelligence systems in medicine is considered in the example of the USA, EU and Singapore. Each country is endeavoring to strike a balance between the protection of personal data privacy and the advancement of technological innovations. The analysis suggests that the emphasis on artificial intelligence development necessitates specific premises in the domain of personal data protection. Conversely, stringent standards for the protection of personal data could potentially exert a restrictive influence.
Keywords: artificial intelligence, AI, health data, Big Data, privacy data protection.
For citation: Galkina, N., Kuznetsova, D. (2024) Regulation and protection of personal health data in the AI era: international experience. *Theoretical and Applied Law,* no. 3 (21), pp. 96–106. (In Russ.) DOI: 10.22394/3034-2813-2024-3-96-106

Цифровизация государства и общества, внедрение новых технологий во все сферы жизни привели к оптимизации многих процессов. Жизнь человека стала быстрее, проще и удобнее. Появление искусственного интеллекта (далее — ИИ) продвинуло человечество еще дальше на пути цифровой трансформации, спровоцировав новый огромный скачок в развитии. На сегодняшний день ИИ активно захватывает сферу за сферой, и особые успехи и достижения можно видеть в сфере медицины и медицинских технологий[1]. Использование ИИ в медицине расширяет возможности диагностики, лечения и исследований. Это и использование ИИ для анализа медицинских снимков с целью оказания помощи врачам для принятия решений, и разработки в области предиктивной медицины[2]. Однако внедрение ИИ ставит много вопросов как практического, так и этического характера. Одним из основных является вопрос обращения с персональными данными. Обучение систем ИИ требует больших объемов данных. Для разработки и использования ИИ в медицине ключевую роль играет доступ к данным пациентов.

Медицинские данные относятся к специальной категории персональных данных, требующей особой защиты[3]. Одним из способов использования таких данных может быть их предварительная анонимизация[4].

По общему правилу анонимизированные персональные данные не подпадают под действие законов о защите конфиденциальности персональных данных. Таким образом, ключевым моментом в контексте анонимизации является исключение возможности повторной идентификации.

При использовании медицинских персональных данных системами ИИ существует высокий риск деанонимизации[5]. Это связано с развитием систем ИИ, с совершенствованием алгоритмов, с тем, что ИИ становится «умнее». Способность ИИ находить закономерности может привести к непреднамеренному раскрытию информации. Помимо повторной идентификации, ИИ также способен делать сложные предположения о данных, не связанных со здоровьем[6]. Всё это представляет угрозу конфиденциальности персональных данных.

---

[1] Как искусственный интеллект меняет будущее медицины. Forbes. URL: https://www.forbes.ru/mneniya/488597-kak-iskusstvennyj-intellekt-menaet-budusee-mediciny (дата обращения: 09.04.2024).

[2] См.: *Raz M., Nguyen T. C., Loh E.* (2023) Artificial Intelligence in Medicine. *Springer*. DOI: https://doi.org/10.1007/978-981-19-1223-8
См.: Алексеева М. Г. Искусственный интеллект в медицине / М. Г. Алексеева, А. И. Зубов, М. Ю. Новиков // Международный научно-исследовательский журнал. 2022. № 7-2 (121). С. 10–13. DOI: 10.23670/IRJ.2022.121.7.038. EDN: JMMMDF

[3] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» относит данные о состоянии здоровья к специальной категории персональных данных (ст. 10). Такой же логике следует европейский GDPR.

[4] См.: *Stam A., Kleiner B.* (2020) Data anonymisation: legal, ethical, and strategic considerations. *FORS Guide No. 11, Version 1.0*. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS, 2020. DOI: 10.24449/FG-2020-00011

[5] См.: *Murdoch B.* (2021) Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*. DOI: https://doi.org/10.1186/s12910-021-00687-3

[6] См.: *Price II W. N.* (2021) Problematic Interactions between AI and Health Privacy. Utah L. Rev. U of Michigan Public Law Research Paper. No. 21-014. Доступно на SSRN: https://ssrn.com/abstract=3797161 (дата обращения: 12.04.2024).

В теории анонимизация данных кажется идеальным решением, но на практике не всегда соответствует ожиданиям, не только из-за рисков повторной идентификации, но и из-за утраты потенциала информативности данных. Между тем качество данных имеет ключевое значение для развития ИИ[1]. Анализ больших массивов информации, особенно с использованием алгоритмов, нацелен на выявление скрытых закономерностей и связей между данными. Однако цель анонимизации — исключить возможность идентификации личности, убрав эти связи. Это создает дилемму: как сделать данные анонимными, сохраняя их ценность для анализа и предоставления третьим сторонам. В этой связи крайне важно найти баланс между защитой конфиденциальности персональных данных и развитием инноваций. В разных странах этот вопрос решается по-разному. Потому анализ зарубежного опыта представляется интересным.

В рамках настоящей статьи на примере США, ЕС и Сингапура будет рассмотрен опыт в сфере правового регулирования обращения с медицинскими персональными данными при использовании систем искусственного интеллекта в медицине.

Европейский союз (ЕС)

В 2014 г. Рабочая группа по защите данных в рамках ст. 29 Европейского союза выпустила заключение по методам анонимизации данных[2]. Это заключение направлено на обеспечение соответствия обработки данных требованиям Общего регламента ЕС по защите персональных данных (GDPR).

Заключение соответствует директивам ЕС о защите данных и подчеркивает, что при оценке риска повторной идентификации необходимо учитывать все возможные средства, которые могут быть разумно применены как контролером, так и любой третьей стороной. Также в документе подтверждается, что, хотя анонимные данные не подпадают под действие законов о защите данных, сам процесс анонимизации является формой обработки персональных данных[3].

Документ устанавливает высокий порог для критериев анонимности, так, чтобы деидентифицированные данные не могли быть повторно идентифицированы ни контролером данных, ни другими сторонами. Этот процесс включает в себя различные методы, каждый из которых адаптирован к конкретным условиям использования данных.

Одним из таких методов является *рандомизация*, которая основана на изменении данных для разрыва связи между персональными данными и физическим лицом, при этом сохраняется полезность данных для контролера.

Второй метод — *обобщение* — направлен на сокращение детализации данных, что снижает риск раскрытия информации о субъекте данных. Применение этого метода делает менее вероятным выделение отдельных физических лиц, особенно когда данные нескольких субъектов консолидируются. Примером может служить агрегирование категорий половой принадлежности в базе данных, что предотвращает идентификацию конкретных лиц.

Третий метод — *маскировка* — часто используется в сочетании с другими техниками анонимизации. Он включает в себя удаление таких идентификаторов из данных, как имена, изображения и адреса. Однако сама по себе маскировка обычно недостаточна для полной анонимизации, поэтому необходимо использовать другие методы защиты персональных данных.

С точки зрения права обработка персональных данных с целью их анонимизации по-прежнему требует наличия законного основания в соответствии со ст. 6 GDPR. Анонимизация, как дальнейшая обработка данных, должна соответствовать принципу ограничения цели. Чаще всего основаниями для контролеров

---

[1] См.: *Matheny M., Israni S. T., Ahmed M., Whicher D.* (2022) Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril. Washington, DC: National Academy of Medicine.

[2] Рабочая группа Европейской комиссии по защите персональных данных (Рабочая группа по статье 29). (2014). Мнение 05/2014 о методах анонимизации.

[3] См.: *Emam K., Alvarez C.* (2014) A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. *International Data Privacy Law*. Vol. 5, no. 1. Pp. 73–87. DOI: 10.1093/idpl/ipu033

или обработчиков данных служат выполнение договорных условий или законные интересы, если соблюдены принципы сбора, целей и сроков хранения данных[1].

Если анонимизация выполнена корректно, данные больше не связаны с конкретным физическим лицом и не рассматриваются как персональные данные в рамках GDPR. Это означает, что такие данные можно использовать свободно. Процесс анонимизации может способствовать улучшению соответствия организации требованиям по защите данных, включая стратегии «конфиденциальности по умолчанию» и «минимизации данных», что позволяет использовать данные без риска причинения вреда субъектам данных.

Следует отметить, что GDPR имеет прямую юридическую силу во всех государствах, членах ЕС, и распространяется на всех граждан ЕС. Тем не менее GDPR предоставляет государствам, членам Европейского союза, возможность вносить некоторые исключения, связанные с общественными интересами и научными исследованиями, что приводит к разнообразию подходов к управлению и защите данных на национальном уровне[2]. В контексте GDPR страны-члены имеют право самостоятельно определять, какие методы псевдонимизации считать адекватными, устанавливать критерии для полной анонимизации данных, вводить специфические ограничения на обработку конфиденциальных данных в исследовательских целях и определять условия, при которых данные могут быть освобождены от ограничений для использования в научных исследованиях[3]. Что касается медицинских данных, то, согласно GDPR, они относятся к специальным категориям персональных данных, требующих более внимательного обращения и более надежной защиты ввиду их чувствительности[4]. Поэтому основным способом их использования для ИИ в медицине является полная предварительная анонимизация.

Всё более активное использование технологий ИИ в здравоохранении выявляет риски для конфиденциальности и защиты данных пациентов, в том числе несанкционированное повторное использование данных, утечки и угрозы кибератак[5].

Далее, 13 марта 2024 г. Европарламент одобрил Закон Европейского союза об искусственном интеллекте (EU AI Act)[6]. Предполагается, что данный закон, как и GDPR, станет глобальным стандартом. Системы ИИ делятся на три категории в зависимости от степени риска: 1) недопустимый риск, 2) высокий риск и 3) низкий или минимальный риск. Системы ИИ, которые принадлежат к категории недопустимого риска, нарушают фундаментальные ценности Европейского союза и, следовательно, должны быть запрещены. Медицинские технологии, основанные на ИИ, классифицируются как технологии высокого риска. Использование таких технологий может быть разрешено только в случае, если они соответствуют строгим требованиям управления рисками, включая обеспечение контроля со стороны человека и проведение постмаркетингового мониторинга[7]. Также закон предусматривает, что для разработки систем ИИ высокого риска субъекты, включая поставщиков, нотифицированные органы и другие заинтересованные организации, такие как центры цифровых инноваций, экспериментальные испытательные центры и научные исследователи, должны обладать возможностью доступа к высококачественным наборам данных для их использования в соответствующих сферах деятельности. И прямо закреплено, что «например, в здравоохранении европейское пространство данных о здоровье будет способствовать недискриминационному

---

[1] См.: *Чурилов А. Ю.* Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Вестник Омской юридической академии. 2019. Т. 16, № 1. С. 29–35. DOI: 10.19073/2306-1340-2019-16-1-29-35. EDN: ZAYHTV

[2] См.: Доступ к медицинским данным: обработка данных в медицинской отрасли. Экономика. Аналитический отчет, ноябрь 2022 г.

[3] См.: *Bak M., Madai V. I., Fritzsche M.-C., Mayrhofer M. T., McLennan S.* (2022) You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly. *Frontiers in Genetics*. DOI: 10.3389/fgene.2022.929453

[4] Art. 9 GDPR:Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

[5] См.: Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts. STUDY Panel for the Future of Science and Technology. European Parliamentary Research Service Scientific Foresight Unit (STOA). PE 729.512. June 2022. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf (дата обращения: 14.04.2024).

[6] The EU AI Act. URL: https://www.euaiact.com/ (дата обращения: 15.04.2024).

[7] Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts. STUDY Panel for the Future of Science and Technology. European Parliamentary Research Service Scientific Foresight Unit (STOA). PE 729.512. June 2022. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729512/EPRS_STU(2022)729512_EN.pdf (дата обращения: 14.04.2024).

доступу к данным о здоровье и обучению алгоритмов искусственного интеллекта на этих наборах данных, с сохранением конфиденциальности, безопасно, своевременно, прозрачно и надежно, а также при соответствующем институциональном управлении. Соответствующие компетентные органы, в том числе отраслевые, предоставляющие или поддерживающие доступ к данным, могут также поддерживать предоставление высококачественных данных для обучения, проверки и тестирования систем искусственного интеллекта»[1].

GDPR отличается особой строгостью, и потому в ЕС вопрос поиска баланса между защитой данных и развитием инноваций стоит особенно остро. Более либеральный подход может иметь серьезные последствия для фундаментальных прав на неприкосновенность частной жизни. В то же время ограничительный подход может тормозить развитие ИИ в медицине и ставить под сомнение эффективность инвестирования в эту сферу. Нормативные акты, регулирующие использование ИИ, должны обладать необходимой гибкостью и адаптироваться к требованиям общества и изменениям в научно-техническом прогрессе. В настоящее время пункт g ст. 9 GDPR представляет собой правовую основу для возможности использования неанонимизированных медицинских данных системами ИИ: в нем указано, что запрет на обработку медицинских данных не применяется, если обработка необходима по причинам, представляющим значительный общественный интерес, на основании законодательства Союза или государства-члена, которые должны быть соразмерны преследуемой цели, уважать суть права на защиту данных и предусматривать надлежащие и конкретные меры по защите основных прав и интересов субъекта данных[2].

Соединенные Штаты Америки

В контексте защиты персональных данных и анонимизации в Соединенных Штатах действует ряд федеральных законодательных актов, которые регламентируют вопросы конфиденциальности и безопасности личной информации в различных секторах экономики. Основным законом, регулирующим вопросы конфиденциальности медицинских данных, является Закон о преемственности и подотчетности медицинского страхования (Health Insurance Portability and Accountability Act, HIPAA). HIPAA устанавливает строгие требования к защите идентифицируемой медицинской информации (PHI), которые касаются не только конфиденциальности, но и целостности и доступности электронной медицинской информации.

Согласно HIPAA, PHI включает в себя любую информацию о состоянии здоровья, медицинских услугах и платежах за них, которая может быть связана с конкретным человеком. HIPAA состоит из нескольких различных частей, также известных как «правила», которые касаются различных аспектов управления медицинской информацией. Правило конфиденциальности (Privacy Rule) устанавливает стандарты защиты медицинской информации, ограничения и условия использования и раскрытия такой информации без разрешения пациента. Правило безопасности (Security Rule) дополняет Правило конфиденциальности и устанавливает стандарты для защиты конфиденциальности, целостности и доступности электронной защищенной медицинской информации.

Один из способов обеспечения защиты PHI — деидентификация данных. HIPAA определяет два метода деидентификации: метод экспертного определения и метод «безопасной гавани». Метод экспертного определения предусматривает привлечение высококвалифицированного специалиста, который подтверждает невозможность использования информации для идентификации физического лица. Этот эксперт применяет специализированные методики и фиксирует процесс деидентификации данных в документальной форме. Метод «безопасной гавани» заключается в исключении из данных ряда конкретных идентификаторов, таких как имя, адрес, дата рождения и другие уникальные числа или коды.

Важно отметить, что деидентификация в HIPAA не равносильна анонимизации в понимании таких норм, как GDPR в Европейском союзе. В то время как GDPR требует удаления возможности идентификации лица для анонимизации, деидентификация по HIPAA, скорее, соответствует псевдонимизации,

[1] The EU AI Act. URL: https://www.euaiact.com/ (дата обращения: 15.04.2024).
[2] 9 (g) GDPR. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 (дата обращения: 16.04.2024).

где данные не могут быть связаны с лицом без дополнительной информации. При этом деидентифицированные данные не являются персональными и не подпадают под соответствующее регулирование. Таким образом, можно отметить, что HIPAA является менее строгим, нежели GDPR, поскольку предъявляет более мягкие требования к анонимизации данных.

В контексте расширения использования цифровых технологий и их интеграции в медицинскую практику такие устройства, как фитнес-браслеты и мобильные приложения, которые собирают медицинские данные, часто остаются за рамками HIPAA, создавая потенциальные угрозы конфиденциальности данных. Это подчеркивает необходимость дальнейшего развития законодательной базы для охвата новых технологий и методов обработки данных в здравоохранении[1]. Попытки решить этот вопрос делаются на уровне штатов. Так, 27 апреля 2023 г. был принят Закон штата Вашингтон «О моем здоровье и моих данных»[2]. Этот закон предназначен для регулирования обработки медицинских данных физических лиц, которые не охватываются действием HIPAA. Особенностью этого законодательного акта является широкое толкование термина «данные о состоянии здоровья потребителей» (consumer health data, CHD), под которым подразумеваются не только данные, непосредственно касающиеся здоровья пациента, но и множество других сведений, не связанных непосредственно со здоровьем. Включение их в это понятие, подлежащее защите закона, мотивировано тем, что их можно связать с медицинскими данными пациента, а это может нарушить конфиденциальность. «CHD определяется в широком смысле как информация, которая связана или может быть разумно связана с потребителем и которая идентифицирует прошлое, настоящее или будущее состояние физического или психического здоровья потребителя»[3]. Закон содержит требования к обращению и конфиденциальности CHD, по строгости подобные европейскому GDPR, это и получение согласия субъекта данных, и жесткие правила по сбору, передаче данных. Также широким является перечень организаций, на которые закон распространяет свое действие, и ввиду широкого понимания CHD это не только организации сферы здравоохранения. Закон штата Вашингтон служит моделью для других штатов. Подобный закон, посвященный регулированию медицинских данных, уже вступил в силу в штате Невада[4].

В октябре 2023 г. президент США Джо Байден издал указ «О безопасном, надежном и заслуживающем доверия развитии и использовании искусственного интеллекта». В нем подчеркивается важность безопасности ИИ, защиты частной жизни и справедливого использования технологий ИИ.

Как указано в документе, «искусственный интеллект облегчает извлечение, повторную идентификацию, установление связей, выводы и действия с конфиденциальной информацией о личности, местонахождении, привычках и желаниях людей. Возможности искусственного интеллекта в этих областях могут увеличить риск использования и раскрытия персональных данных. Для борьбы с этим риском федеральное правительство будет обеспечивать законность сбора, использования и хранения данных, их безопасность и снижение рисков, связанных с неприкосновенностью частной жизни и конфиденциальностью»[5]. Указ президента США для продвижения инноваций в сфере ИИ в медицине предусматривает выделение средств на инициативы, изучающие пути повышения качества данных в здравоохранении и поддержку разработки инструментов ИИ для клинического лечения, здоровья населения, общественного здравоохранения и исследований в этой области.

Регулирование ИИ в США можно охарактеризовать как «мягкий подход», целью которого является стимулирование инноваций[6].

---

1 См.: *Price W., Cohen I.* (2019) Privacy in the age of medical big data. *Nature Medicine*. Pp. 37–43. DOI: https://doi.org/10.1038/s41591-018-0272-7

2 My health My data Act. URL: https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230503092232 (дата обращения: 12.04.2024).

3 Sec. 3 part 8 (a). URL: https://lawfilesext.leg.wa.gov/biennium/2023-24/Pdf/Bills/Session%20Laws/House/1155-S.SL.pdf?q=20230503092232 (дата обращения: 16.04.2024).

4 Закон штата Невада о конфиденциальности данных о здоровье потребителей, Senate Bill 370.

5 Section 2 (f). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ (дата обращения: 15.04.2024).

6 См.: *Ли Я.* Нормативно-правовое регулирование генеративного искусственного интеллекта в Великобритании, США, Европейском союзе и Китае // Право. Журнал Высшей школы экономики. 2023. № 3. С. 245–267. DOI: 10.17323/2072-8166.2023.3.245.267. EDN: YITZOA

Сингапур

Сингапур — один из мировых лидеров в области технологий и инноваций, поэтому также уделяет особое внимание вызовам, связанным с защитой персональных данных в эпоху глобальной цифровизации.

Разработка и принятие Закона о защите персональных данных (PDPA) в 2012 г., а затем внесение в него поправок в 2020 г. стали ответом на необходимость модернизации правового поля в условиях растущей цифровизации. Особое внимание в этом контексте уделяется анонимизации данных — процессу, который позволяет использовать значительные объемы информации для аналитики и разработки новых продуктов без ущерба для конфиденциальности личной информации. Важно отметить, что в Сингапуре понятия «анонимизация» и «деидентификация» не являются тождественными. PDPC понимает под «деидентификацией» только удаление прямых идентификаторов. При этом деидентифицированный набор данных может быть легко повторно идентифицирован при объединении с данными, которые могут быть общедоступными или легкодоступными. Таким образом, это, по сути, является псевдонимизацией в терминах европейского GDPR. Ключевое значение анонимизации заключается в правовых последствиях этого процесса — анонимизированные данные больше не являются персональными данными для целей PDPA. Полностью анонимизированные данные, когда анонимизация становится необратимой, могут быть открыты для публичного доступа (например, открытые данные).

Правовая база Сингапура в части PDPA четко регламентирует процесс анонимизации, подчеркивая ее значение для защиты прав субъектов данных[1]. Закон не только определяет, какие данные считаются анонимизированными, но и освобождает такие данные от обязательств по защите, предусмотренных для обычных персональных данных. Такой подход предоставляет организациям возможности для использования анонимизированных данных в рамках исследовательских, статистических и маркетинговых проектов без необходимости соблюдения ограничений, которые обычно налагаются на обработку персональных данных[2].

Однако процесс анонимизации сопряжен с определенными рисками, главный из которых — возможность повторной идентификации. В свете этого PDPA вводит строгие требования к методам анонимизации, а также предусматривает ответственность за несанкционированную повторную идентификацию анонимизированных данных. Организациям, работающим с анонимизированными данными, необходимо регулярно проводить оценку рисков и принимать меры для обеспечения того, чтобы данные невозможно было связать с конкретными лицами.

Практические руководства и стандарты, разработанные Комиссией по защите персональных данных Сингапура (PDPC), предоставляют детальные указания по вопросам анонимизации, включая описание техник и методов, которые могут быть использованы для обеспечения соответствия анонимизированных данных требованиям законодательства. Такие документы, как Руководство по базовой анонимизации, являются важными инструментами для организаций, стремящихся управлять данными в соответствии с законом.

Необходимо отметить, что PDPA не содержит определения «чувствительных данных» (sensitive data), он применяется ко всем типам персональных данных. Тем не менее некоторые типы данных, к которым относятся и данные о здоровье, считаются чувствительными в силу их характера и потенциального вреда, который может быть причинен в результате их неправильного использования. По этой причине Комиссия по защите персональных данных (Personal Data Protection Commission, PDPC) в выпущенном совместно с Министерством здравоохранения Консультативном руководстве для сектора здравоохра-

[1] PDPA содержит в своем тексте упоминание анонимизированной информации, однако не содержит прямого определения таких данных и «анонимизации». Подробную информацию и определения можно найти в гл. 3 Консультативных руководств по PDPA для отдельных тем, выпущенных PDPC, которая посвящена вопросам анонимизации. Advisory Guidelines on the Personal Data Protection Act for Selected Topics. Advisory Guidelines on the Personal Data Protection Act for Selected Topics. URL: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-17-May-2022.pdf (дата обращения: 16.04.2024).

[2] См.: Цифровая трансформация и государственное управление: научно-практическое пособие / *А. С. Емельянов*, *А. А. Ефремов*, *А. В. Калмыкова* и др.; ред. кол.: *Л. К. Терещенко*, *А. С. Емельянов*, *Н. А. Поветкина*. М.: Инфотропик Медиа, 2022. 224 с.

нения[1] рекомендует проявлять повышенную осторожность при работе с персональными медицинскими данными, учитывая потенциальные последствия нарушения их конфиденциальности для частной жизни физических лиц. Кроме того, в PDPC закреплена строгая позиция при рассмотрении случаев, когда скомпрометированные персональные данные носят чувствительный характер.

Правительство Сингапура определило ИИ как одну из основных передовых технологий, которые необходимы для развития цифровой экономики страны[2]. 1 марта 2024 г. PDPC выпустила Консультативное руководство по использованию персональных данных в рекомендательных системах и системах принятия решений на базе ИИ[3]. В Руководстве указано, что оно применяется ко всем видам сбора и использования персональных данных организацией, включая сбор и/или обработку персональных данных для разработки, тестирования и мониторинга систем ИИ. В дополнение к получению согласия на использование персональных данных для обучения систем ИИ организации могут также рассматривать возможность использования персональных данных без согласия на основании таких исключений, как «совершенствование бизнес-процессов» (актуально, когда организация разработала новый продукт или совершенствует уже существующий)[4] или «исследования» (когда организация проводит коммерческие исследования для развития науки и техники без разработки дорожной карты развития продукта)[5]. Важно отметить, что PDPC в своем Руководстве не ограничивает организации использованием только анонимизированных данных, наоборот, ввиду того, что использование анонимизированных данных сопряжено с определенными компромиссами, рекомендуется тщательно взвесить все плюсы и минусы использования обоих типов данных (анонимизированных и персональных) и четко документировать их.

Таким образом, анонимизация данных в Сингапуре — это не только техническая, но и юридическая необходимость, позволяющая сочетать инновационное использование данных с обязательствами по их защите. В управлении ИИ, в отличие от других юрисдикций, Сингапур демонстрирует бо́льшую сбалансированность[6]. При этом важно отметить, что сингапурский подход к использованию персональных данных системами ИИ представляет собой гибкий подход, который стимулирует технологическое развитие и одновременно защищает права граждан.

Подведем итог: в рамках сравнительно-правового анализа законодательств о защите данных в Европейском союзе, США и Сингапуре особенное внимание следует уделить различиям в подходах к анонимизации данных. Эти различия отражают как общие цели законодательства, так и специфические правовые и культурные контексты каждой юрисдикции.

Общий регламент по защите данных (GDPR) Европейского союза является комплексным законодательным документом, цель которого заключается в укреплении и гармонизации механизмов защиты персональных данных в государствах, членах ЕС. GDPR направлен не только на защиту персональных данных, но также на обеспечение свободы их циркуляции внутри Европейского союза. Регламент вводит строгие требования к анонимизации данных, разграничивая ее от псевдонимизации и требуя необратимого удаления любых возможностей для идентификации личности.

Федеральный закон HIPAA в США, в свою очередь, сфокусирован на защите медицинской информации. Хотя HIPAA также включает положения по деидентификации данных, этот процесс менее строгий по сравнению с GDPR и направлен на удаление определенных идентификаторов, что позволяет считать

---

1 Advisory Guidelines for the Healthcare Sector. URL: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-for-the-healthcare-sector-sep-2023.pdf (дата обращения: 16.03.2024).

2 National Artificial Intelligence Strategy. URL: https://file.go.gov.sg/nais2019.pdf (дата обращения: 16.04.2024).

3 Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. URL: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/advisory-guidelines/advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf (дата обращения: 14.04.2024).

4 Division 2 under Part 2 of the Second Schedule to the PDPA. Business improvement purpose. URL: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=Sc2-#Sc2- (дата обращения: 14.04.2024).

5 Division 3 under Part 2 of the Second Schedule to the PDPA. Research. URL: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=Sc2-#Sc2- (дата обращения: 14.04.2024).

6 *Walters R., Coghlan M.* (2019) Data Protection and Artificial Intelligence Law: Europe Australia Singapore — An Actual or Perceived Dichotomy. *American Journal of Science, Engineering and Technology*. Vol. 4, No. 4. P. 58. DOI: 10.11648/j.ajset.20190404.11

данные деидентифицированными, но не полностью анонимизированными в европейском понимании этого термина.

В Сингапуре Закон о защите персональных данных (PDPA) определяет принципы обработки персональных данных в частном и государственном секторах. Аналогично закону HIPAA, PDPA включает положения об анонимизации данных как о мере защиты, предоставляя при этом возможности для гибкого использования анонимизированных данных в коммерческих целях. Такой подход демонстрирует стремление Сингапура к достижению баланса между защитой данных и потребностями динамично развивающейся цифровой экономики.

Сравнивая эти три подхода, можно заметить, что GDPR представляет наиболее строгую и всестороннюю систему защиты данных, акцентирующую внимание на правах субъектов данных и контроле над их персональной информацией. HIPAA, будучи ограниченным сферой здравоохранения, предоставляет более специализированные инструменты для защиты медицинской информации, тогда как PDPA более гибок и адаптивен к потребностям коммерческой деятельности.

Развитие ИИ построено на обработке большого массива данных. Данные — это, по сути, пища для систем ИИ. И чем более полные данные, тем зачастую интереснее предлагаемые технологические решения и шире возможности систем ИИ. Создание полностью анонимизированных датасетов не всегда отвечает нуждам разработчиков. Таким образом, строгость стандартов защиты персональных данных становится значительным барьером для реализации множества технологических инициатив. Противоречие между защитой персональных данных и развитием искусственного интеллекта на данный момент представляет собой одну из ключевых проблем, требующих адекватного разрешения. Потому каждая юрисдикция пытается найти свое сочетание строгости и уступок, чтобы достигнуть того самого баланса развития инноваций и защиты конфиденциальности. Если говорить об использовании ИИ в медицине, то тут все эти противоречия проявляются особенно остро, поскольку, вне зависимости от выделения медицинской информации в отдельную категорию законами о защите конфиденциальности персональных данных или отсутствия такового, медицинские персональные данные являются особенно чувствительными, и их несанкционированное раскрытие и ненадлежащее использование могут причинить особо ощутимый вред. В то же время внедрение ИИ именно в сферу медицины может принести жизненно важную пользу: персонализация медицинской помощи, повышение эффективности ее оказания будут способствовать улучшению качества жизни и ее продолжительности, что является стратегической задачей каждого государства.

Таким образом, государства стоят перед серьезной дилеммой. Если нужны инновации, то придется снижать уровень защиты конфиденциальности, предусматривать определенные «лазейки» и исключения для разработчиков систем ИИ. Опыт Сингапура как раз демонстрирует такой подход, поскольку PDPA делает анонимизацию не единственным решением, предоставляя определенные возможности разработчикам систем ИИ.

Думается, что в связи с очевидной необходимостью определенных допущений, связанных со снижением защиты персональных данных, ключевым решением должно стать усиление защитных мер и глубокая перестройка всех систем безопасности для этих целей. Нельзя не согласиться, что «частные компании, работающие с данными, могут быть подвержены влиянию конкурирующих целей и должны структурно поощряться для обеспечения защиты данных и предотвращения их альтернативного использования»[1]. Должны иметь место постоянное тестирование систем на уязвимость, проверка блоков анонимизированной информации на возможность повторной идентификации, строгая фиксация целей и способов обращения с неанонимизированной информацией и особо строгие правила и механизмы работы с ней на уровне компаний, жесткий контроль за этим со стороны регуляторов. И отдельное внимание, полагаем, должно быть уделено усилению наказаний за утечки информации. Крупные оборотные штрафы для компаний, не соблюдающих установленные требования по обеспечению безопасности данных, должны быть экономическим стимулом для совершенствования корпоративных

[1] *Murdoch B.* Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics*, 2021. No. 22 P. 1. https://doi.org/10.1186/s12910-021-00687

политик с целью обеспечения максимального уровня безопасности. Компании должны вкладывать деньги в совершенствование систем безопасности с целью купирования всех возможных рисков.

Литература

1. *Алексеева М. Г.* Искусственный интеллект в медицине / М. Г. Алексеева, А. И. Зубов, М. Ю. Новиков // Международный научно-исследовательский журнал. 2022. № 7-2 (121). С. 10–13. DOI: 10.23670/IRJ.2022.121.7.038. EDN: JMMMDF
2. *Ли Я.* Нормативно-правовое регулирование генеративного искусственного интеллекта в Великобритании, США, Европейском союзе и Китае // Право. Журнал Высшей школы экономики. 2023. № 3. С. 245–267. DOI: 10.17323/2072-8166.2023.3.245.267. EDN: YITZOA
3. *Чурилов А. Ю.* Принципы Общего регламента Европейского союза о защите персональных данных (GDPR): проблемы и перспективы имплементации // Вестник Омской юридической академии. 2019. Т. 16, № 1. С. 29–35. DOI: 10.19073/2306-1340-2019-16-1-29-35. EDN: ZAYHTV
4. *Bak M., Madai V. I., Fritzsche M.-C., Mayrhofer M. T., McLennan S.* (2022) You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly. *Frontiers in Genetics*. DOI: 10.3389/fgene.2022.929453
5. *Emam K., Alvarez C.* (2014) A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. *International Data Privacy Law*. Vol. 5, no. 1. Pp. 73–87. DOI: 10.1093/idpl/ipu033
6. *Matheny M., Israni S. T., Ahmed M., Whicher D.* (2022) Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril. Washington, DC: National Academy of Medicine, 2022.
7. *Murdoch B.* (2021) Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*. DOI: https://doi.org/10.1186/s12910-021-00687-3
8. *Price II W. N.* (2021) Problematic Interactions between AI and Health Privacy. 2021 Utah L. Rev. U of Michigan Public Law Research Paper No. 21-014. Доступно на SSRN: https://ssrn.com/abstract=3797161 (дата обращения: 12.04.2024).
9. *Price W., Cohen I.* (2019) Privacy in the age of medical big data. Nature Medicine. Pp. 37–43. DOI: https://doi.org/10.1038/s41591-018-0272-7
10. *Raz M., Nguyen T. C., Loh E.* (2023) Artificial Intelligence in Medicine. Springer. DOI: https://doi.org/10.1007/978-981-19-1223-8
11. *Stam A., Kleiner B.* (2020) Data anonymisation: legal, ethical, and strategic considerations. *FORS Guide No. 11, Version 1.0*. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS, 2020. DOI: 10.24449/FG-2020-00011
12. *Walters R., Coghlan M.* (2019) Data Protection and Artificial Intelligence Law: Europe Australia Singapore — An Actual or Perceived Dichotomy. *American Journal of Science, Engineering and Technology*. Vol. 4, No. 4. Pp. 55–65. DOI: 10.11648/j.ajset.20190404.11

Об авторах:

Галкина Наталия Михайловна, заместитель директора Института исследований национального и сравнительного права факультета права Национального исследовательского университета «Высшая школа экономики» (Москва, Российская Федерация)
e-mail: ngalkina@hse.ru
ORCID: https://orcid.org/0009-0004-6440-3404

Кузнецова Дарья Владимировна, ведущий эксперт института исследований национального и сравнительного права факультета права Национального исследовательского университета «Высшая школа экономики» (Москва, Российская Федерация)
e-mail: dvkuznetsova@hse.ru
ORCID: https://orcid.org/0009-0003-4059-865x

References

1. Alekseeva, M. G., Zubov, A. I., Novikov, M. Yu. (2022) Artificial Intelligence in Medicine. *International Research Journal*. No. 7-2 (121). Pp. 10–13. DOI: 10.23670/IRJ.2022.121.7.038
2. Li, Ya. (2023) Specifics of Regulatory and Legal Regulation of Generative Artificial Intelligence in the UK, USA, EU and China. Law. *Journal of the Higher School of Economics*. Vol. 16, no. 3. Pp. 245–267 (In Russ.). DOI: 10.17323/2072-8166.2023.3.245.267
3. Churilov, A. Yu. (2019) Principles of the EU general regulations for the protection of personal data (GDPR): problems and perspectives for implementation. *Siberian Legal Review.* Vol. 16, No. 1. Pp. 29–35. DOI: 10.19073/2306-1340-2019-16-1-29-35
4. Bak, M., Madai, V. I., Fritzsche, M.-C., Mayrhofer, M. T., McLennan, S. (2022) You Can't Have AI Both Ways: Balancing Health Data Privacy and Access Fairly. *Frontiers in Genetics*. DOI: 10.3389/fgene.2022.929453
5. Emam, K., Alvarez, C. (2014) A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques. *International Data Privacy Law*. Vol. 5, no. 1. Pp. 73–87. DOI: 10.1093/idpl/ipu033
6. Matheny, M., Israni, S. T., Ahmed, M., Whicher, D. (2022) Artificial Intelligence in Health Care: The Hope, the Hype, the Promise, the Peril. Washington, DC: *National Academy of Medicine*.
7. Murdoch, B. (2021) Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*. DOI: https://doi.org/10.1186/s12910-021-00687-3
8. Price II, W. N. (2021) Problematic Interactions between AI and Health Privacy. 2021 Utah L. Rev. U of Michigan Public Law Research Paper No. 21-014. Доступно на SSRN: https://ssrn.com/abstract=3797161 (дата обращения: 12.04.2024).
9. Price, W., Cohen, I. (2019) Privacy in the age of medical big data. Nature Medicine. Pp. 37–43. DOI: https://doi.org/10.1038/s41591-018-0272-7
10. Raz, M., Nguyen, T. C., Loh, E. (2023) Artificial Intelligence in Medicine. Springer. DOI: https://doi.org/10.1007/978-981-19-1223-8
11. Stam, A., Kleiner, B. (2020) Data anonymisation: legal, ethical, and strategic considerations. *FORS Guide No. 11, Version 1.0*. Lausanne: Swiss Centre of Expertise in the Social Sciences FORS, 2020. DOI: 10.24449/FG-2020-00011
12. Walters, R., Coghlan, M. (2019) Data Protection and Artificial Intelligence Law: Europe Australia Singapore — An Actual or Perceived Dichotomy. *American Journal of Science, Engineering and Technology*. Vol. 4, No. 4. Pp. 55–65. DOI: 10.11648/j.ajset.20190404.11

About the authors:

Nataliia M. Galkina, Deputy Director at the Institute of National and Comparative Legal Studies, LL.M, National Research University Higher School of Economics (Moscow, Russian Federation)
e-mail: ngalkina@hse.ru
ORCID: https://orcid.org/0009-0004-6440-3404

Daria V. Kuznetsova, Lead Expert at the Institute of National and Comparative Legal Studies, LL.M, National Research University Higher School of Economics (Moscow, Russian Federation)
e-mail: dvkuznetsova@hse.ru
ORCID: https://orcid.org/0009-0003-4059-865x