УДК 342, 349 DOI: 10.31249 /iajpravo/2026.04.11

ФЕДОТОВ Н.Е.[1] ПРАВОВАЯ ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ЗДРАВООХРАНЕНИЯ: ОПЫТ РОССИИ, КИТАЯ И ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. В статье исследуются ключевые проблемы, возникающие при реализации права на неприкосновенность частной жизни, в том числе, угрозы нарушения обработки «чувствительных» персональных данных в здравоохранении с помощью информационных технологий. Особое внимание уделено опыту Китайской Народной Республики, где приняты меры по минимизации сбора медицинских данных в мобильных приложениях из числа технологий Интернета вещей. Обоснована целесообразность внедрения в российское законодательство механизма оценки степени риска причинения вреда субъекту данных, создания динамического перечня приложений с дифференцированными требованиями к составу обрабатываемой конфиденциальной персональной информации.

Ключевые слова: цифровизация здравоохранения; информационные технологии; неприкосновенность частной жизни; технологии искусственного интеллекта; технологии Интернета вещей; правовое регулирование; персональные данные.

FEDOTOV N.E. Legal Protection of Sensitive Personal Data in the Context of Healthcare Digitalisation: the Experience of Russia, China, and the European Union

Abstract. This article examines key issues arising in the exercise of the right to privacy, particularly the risks of violations involving the

[1] © *Федотов Никита Егорович*, кандидат юридических наук, администратор проекта Проектного управления по реализации мероприятий в области развития отрасли информационных технологий ФГБУ «Центр экспертизы и координации информатизации».

processing of “sensitive” personal data in the healthcare sector through the use of information technology. Particular attention is paid to the experience of the People’s Republic of China, where measures have been taken to minimize the collection of medical data in mobile applications that utilize Internet of Things technologies. The paper justifies the advisability of introducing into Russian legislation a mechanism for assessing the degree of risk of harm to data subjects, as well as creating a dynamic list of applications with differentiated requirements regarding the types of confidential personal information processed.

Keywords: digitalisation of healthcare; information technology; privacy; artificial intelligence; Internet of Things technology; legal regulation; personal data.

Для цитирования: Федотов Н.Е. Правовая защита конфиденциальных персональных данных в условиях цифровизации здравоохранения: опыт России, Китая и Европейского союза (Статья) // Социальные и гуманитарные науки. Отечественная и зарубежная литература: ИАЖ. Сер. 4: Государство и право. – 2026. – № 4. – С. 135–146. – DOI: 10.31249 /iajpravo/2026.04.11

Введение

Современные технологии открывают широкие возможности в сфере здравоохранения. Искусственный интеллект (далее – ИИ) анализирует симптомы, данные анализов и историю пациента, подсказывает возможные диагнозы, предупреждает о несовместимости лекарств или возможных аллергических реакциях. Это служит «вторым мнением», снижая риск врачебной ошибки. Также ИИ можно использовать после проведения лечения пациента для прогнозирования вероятности выживаемости, рецидива или осложнений у пациентов через определенный временной промежуток.

Анализ обезличенных медицинских данных населения позволяет выявлять закономерности распространения инфекций, предсказывать вспышки эпидемий и планировать закупки вакцин. Это ключевой инструмент для перехода от лечения к профилактике.

Вся история болезни, результаты анализов, снимки МРТ/КТ и назначения врачей хранятся в единой цифровой среде. Это избавляет пациента от необходимости носить с собой кипы бумаг и повторно проходить обследования при смене врача или клиники, так как данные доступны мгновенно.

Устройства и приложения на базе технологий Интернета вещей позволяют отслеживать физическую активность, питание, сон, а также напоминают о приеме лекарств, что способствует формированию здорового образа жизни. Тем не менее в связи с внедрением информационных технологий в различные сферы медицинской практики актуализируется ряд проблем, которые необходимо разрешить, в том числе и в области частной жизни.

Конфиденциальность персональных данных в контексте применения цифровых технологий

Создание и активное использование информационных баз данных о гражданах как государственными, так и частными организациями способствует развитию конституционного права на неприкосновенность частной жизни. В результате выявляются новые аспекты личной жизни; при этом информационный аспект становится основным.

Вместе с тем в докладе Верховного комиссара ООН по правам человека еще в 2019 г. отмечалось, что недостаточное регулирование, чрезмерное регулирование и умышленное ненадлежащее использование цифровых технологий приводит к появлению новых угроз и рисков, связанных с разглашением конфиденциальной информации, что отражается в виде нарушения права на неприкосновенность частной жизни[1]. В области применения устройств из числа технологий Интернета вещей такие угрозы приобретают особую значимость: несанкционированный доступ к данным с носимых тонометров или глюкометров, компрометация каналов передачи данных между устройством и облачным сервисом, а также возможность перехвата управления самим устройством позволяют злоумышленнику получить чувствительную информацию о состоянии здоровья в реальном времени. Одной из актуальных проблем в вышеуказанной области является нарушение требований безопасности конфиденциальных персональных данных, которое подрывает доверие к системе здравоохранения.

Среди медицинской информации выделяются «чувствительные» данные о здоровье, которые классифицируются как конфи-

[1] Права человека в цифровой век. Какую роль играют права человека в цифровой век?: Основное выступление Верховного комиссара ООН по правам человека Мишель Бачелет. Нью-Йорк, 17.10.2019 г. – URL: https://www.ohchr.org/ru/2019/10/human-rights-digital-age (дата обращения: 22.07.2026).

денциальные персональные данные[1]. Эти сведения требуют повышенной государственной защиты на законодательном уровне, поскольку относятся к категории личной информации о пациенте, распространение которой в принципе недопустимо. Технологическое развитие существенно расширяет перечень данных, способных раскрыть состояние здоровья: помимо прямых медицинских данных, к «чувствительным» могут быть отнесены рассчитанные алгоритмами индекс массы тела, уровень стресса, качество сна, а также биометрические образцы (фотографии сетчатки глаза, рисунок вен, голосовые отпечатки), собираемые приложениями и устройствами из числа технологий Интернета вещей для идентификации пользователя. Алгоритмы, заложенные в них, способны делать вероятностные выводы о предрасположенности к заболеваниям, которые при этом не являются медицинскими диагнозами, но по сути раскрывают столь же чувствительную информацию.

Общий регламент о защите данных ЕС от 27.04.2016 г. (General Data Protection Regulation) (далее – Общий регламент) не содержит прямых ссылок на «чувствительные» персональные данные. Однако в п. 53 преамбулы Общего регламента определяются специальные категории персональных данных, которые требуют более высокой степени защиты при их обработке в целях, связанных со здоровьем и интересами физических лиц или общества в целом, обеспечения непрерывности медицинского обслуживания или социального обеспечения и трансграничного медицинского обслуживания, безопасности, мониторинга здоровья и предупреждения заболеваний и др., поскольку контекст их обработки может создать значительные риски для основных прав и свобод.

Более того, ст. 9 Общего регламента предусматривает новые правовые основания для обработки «чувствительных» персональных данных, например, если обработка «чувствительных» данных необходима по соображениям общественного интереса в сфере здравоохранения, таким как противодействие серьезным трансграничным угрозам здоровью или обеспечение высоких стандартов качества и безопасности медицинского обслуживания, лекарственных препаратов или медицинских изделий, то на основании законодательства ЕС или государства-члена принимаются соответствующие меры по защите прав и свобод субъекта данных, в том числе профессиональной тайны. Положения Общего регламента

[1] Карцхия А.А. Информационно-правовое обеспечение цифровой экосистемы здравоохранения // Правовая информатика. – 2021. – № 1. – С. 13–23.

допускают параллельное нормотворчество ЕС и государств – членов ЕС. Базовый акт ЕС не обладает свойством полной и исключительной унификации всех аспектов правомерности обработки данных: национальный законодатель правомочен принимать специальные правовые акты, конкретизирующие условия законности применительно к отдельным ситуациям. Национальное регулирование уточняет обстоятельства, при которых обработка признается законной, и детализирует общие принципы, закрепленные в ст. 5 Общего регламента. Подобный механизм нормативной конкретизации позволяет адаптировать европейские стандарты к особенностям национальных правопорядков, не нарушая при этом целостности общеевропейского режима защиты персональных данных.

Европейская директива о защите лиц при обработке персональных данных и о свободном перемещении таких данных от 24.10.1995 г. (Directive 95/46/EU) в ст. 8 запрещает обработку «чувствительных» данных, если не применяются исключения, перечисленные в п. 2 данной статьи. В этой Директиве указаны специальные категории персональных данных, раскрывающие расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения, членство в профсоюзах, а также категории данных, касающихся здоровья или половой жизни.

Как отмечают Д.Дж. Солоу и П.М. Шварц, концепция чувствительных данных показывает, как Европейский союз поддерживает различные категории данных с разными уровнями защиты. Директива выделяет особую категорию данных под названием «чувствительные данные» и предоставляет им более сильную защиту, чем другим типам данных[1].

Законодатели европейских государств используют схожий подход: устанавливают запрет на обработку «чувствительных» данных по умолчанию, предусматривая при этом исчерпывающий список исключений.

В отечественном законодательстве, как и в праве ЕС, «чувствительные» персональные данные признаются особой категорией персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, кото-

[1] Schwartz P.M., Solove D.J. Reconciling personal information in the United States and European Union // California Law Review. – 2014. – P. 877–916.

рые в соответствии со ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 24.06.2025) «О персональных данных» ограничиваются при их обработке, за исключением случаев, предусмотренных ч. 2 и 2.1 указанной статьи.

Отношение к «чувствительным» данным показывает, как законодательство различных стран поддерживает идею о том, что разные уровни обязательств при обработке различных категорий персональных данных могут лучше защитить частную жизнь. Типы персональных данных, подпадающие под указанную категорию, автоматически подчиняются более строгим правилам при обработке независимо от контекста использования. Как правило, требуется письменное согласие в явно выраженной форме. Нельзя собирать такие данные «на всякий случай». Цель должна быть конкретной и легитимной (диагностика, лечение, профилактика). Обработка для рекламы без отдельного прямого согласия запрещена. Врач может обработать «чувствительные» персональные данные без согласия, если пациент без сознания и это необходимо для спасения его жизни. Также обработка возможна для медико-профилактических целей, оценки трудоспособности, врачебной экспертизы без согласия, если это выполняет медработник, обязанный обеспечить сохранение врачебной тайны.

Помимо конфиденциальных медицинских данных защите должны подвергаться любые связанные с ними персональные данные, а также персональные данные участников обмена данными, поставщиков и потребителей данных. Таким образом, безопасность и конфиденциальность медицинской информации должны быть гарантированы не только при хранении данных, но и в процессе обмена и / или предоставления доступа к ним.

Рост значимости поиска мер защиты обработки «чувствительных» персональных данных при использовании информационных технологий, как и их внедрение напрямую затрагивают сферу обработки медицинских сведений и конфиденциальных данных о состоянии здоровья.

В частности, с помощью сложных алгоритмов машинного обучения ИИ осуществляется компьютеризированное выявление и диагностика заболеваний. Этот процесс включает в себя выбор признаков из медицинских изображений, подбор подходящей модели / классификатора и соответствующего алгоритма, а затем обучение ИИ на данных, в результате чего получается требуемый результат, который проверяется медицинским специалистом перед постановкой окончательного диагноза.

Вместе с тем собранные медицинские данные поступают с технологий Интернета вещей: носимых устройств, которые фиксируют состояние здоровья пользователя и данные о его физической активности, с устройств пациентов, собирающих медицинские данные, с устройств для получения диагностических изображений, из онлайн-диагностических инструментов, медицинских исследований, клинических испытаний, фармацевтических исследований и т.д.

Также, чтобы использовать огромные массивы данных с помощью технологии анализа больших данных (Big Data) для поиска лекарств или прогноза эпидемий, «чувствительные» данные должны быть деперсонализированы. Прямые идентификаторы удаляются или заменяются кодом. При этом следует учитывать, что даже информация, которая изначально была создана без какой-либо привязки к лицу, может быть впоследствии путем аналогий отнесена к идентифицируемому лицу посредством технологии анализа больших данных. Важно, чтобы процедура анонимизации была необратимой, поскольку речь идет о «чувствительных» персональных данных.

Вышеуказанное, в свою очередь, актуализирует проблемы правового регулирования оборота «чувствительных» персональных данных. Например, важный вопрос, который еще предстоит решить, заключается в необходимости применения определенных методов обеспечения конфиденциальности и безопасности при работе с массивными медицинскими данными и их анализе, чтобы эффективно удовлетворять высокий спрос на них.

Существующие риски обусловливают необходимость разработки нового, более гибкого подхода к оценке обработки «чувствительных» персональных данных. Лучшей отправной точкой в России могло бы стать требование четкого рассмотрения степени риска причинения вреда людям, который несет в себе предполагаемая обработка персональных данных, и вероятной серьезности этого вреда при условии соответствующих исключений, для сохранения баланса частных и публичных интересов. Это потребует подхода, основанного на ответственности, соразмерной обстоятельствам, включая статус контролирующего лица, субъекта данных и любого обработчика.

Федотов Н.Е.

Меры по защите конфиденциальности персональных данных в здравоохранении Китайской Народной Республики

Китай стал внедрять новые информационные технологии и использовать их в здравоохранении еще в 1990-х годах[1]. Переход на электронное здравоохранение начался в 2009 г., когда китайское правительство решительно взялось за реформу здравоохранения. Оно впервые предложило принять информационные технологии здравоохранения в качестве ключевого направления для стимулирования развития медицинской реформы в марте 2009 г. и продвигало электронные медицинские карты[2]. В 2019 г. в оценке подачи заявок на электронные медицинские карты приняли участие 1874 государственные больницы, что на 110 больше, чем в предыдущем году. Уровень участия достиг 99,36%, что является историческим максимумом[3]. Можно сказать, что информатизация больниц в Китае завершила создание инфраструктуры, предусмотренной Национальной комиссией по здравоохранению.

С начала XXI в. исследования ИИ в Китае добились значительного прогресса в области здравоохранения. Китайский рынок ИИ оценивался в 150 млрд юаней в 2022 г., а к 2025 г. ожидалось, что он будет оцениваться в 400 млрд юаней[4].

Вместе с тем право на неприкосновенность частной жизни в Китае подвержено систематическим нарушениям. Установлено, что в Китае часто происходит раскрытие личной информации, а утечки медицинских данных подрывают доверие общества к обра-

[1] Application of telemedicine in Gansu Province of China / Cai Hui, Wang Hongjing, Guo Tiankang, Bao Guoxian // Public Library of Science One. – 2016. – Vol. 11, N. 6. – P. 1–11. – URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0158026 (дата обращения: 22.07.2026).

[2] Opinions of the CPC Central Committee and the State Council on Deepening the Health Care System Reform. – URL: http://www.china.org.cn/government/scio-press-conferences/2009-04/09/content_17575378.htm (дата обращения: 22.07.2026).

[3] Current Status of the Health Information Technology Industry in China from the China Hospital Information Network Conference: Cross-Sectional Study of Participating Companies / Zhongan Zhang, Xu Zheng, Kai An, Yunfan He, Tong Wang, Ruizhu Zhou, Qilin Zheng, Mingfu Nuo, Jun Liang, Jianbo Lei // JMIR medical informatics. – 2022. – Vol. 10, N 1. – P. 1–14.

[4] Katterbauer K., Cleenewerck L. Artificial Intelligence and its Impact on Healthcare Financing in China–A legal Analysis // Financial Law Review. – 2024. – Vol. 33, N 1. – P. 62–81.

ботке данных[1]. Эти инциденты, а также социально-политическая обстановка, в которой право на неприкосновенность частной жизни обычно подчиняется другим социальным целям, создают препятствия для устойчивого развития медицинского ИИ в Китае. То же самое можно сказать и про мобильные медицинские приложения, которые связаны с электронными медицинскими картами пациентов, записями о состоянии здоровья, информацией о консультациях и данными изображений и сильно зависят от сети и информационных технологий. Если системы кибербезопасности или технической безопасности подвергаются атакам или угрозам, может произойти утечка персональных данных.

В целях решения вышеуказанной проблемы в Китае был принят Закон КНР о защите личной информации от 20.08.2021 г. (Personal Information Protection Law), обеспечивающий последовательную правовую базу для защиты персональной информации, включая медицинские данные. Так, для реализации норм данного Закона было выпущено Положение об объеме необходимой личной информации для общих типов мобильных приложений от 12.03.2021 г. (Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications), в соответствии с которым любой сбор личной информации, получаемой с мобильных медицинских приложений, относящихся к технологиям Интернета вещей, за пределами установленного объема может считаться незаконным[2].

Положение отдельно классифицирует приложения, относящиеся к технологиям Интернета вещей в медицине, которые представлены различными устройствами (фитнес-трекеры, умные браслеты, тонометры, глюкометры с мобильным приложением). Для каждого из них установлен исчерпывающий список данных, которые могут собираться. Например, для условного подобного приложения могут быть включены:

– регистрационные данные (номер мобильного телефона, идентификатор аккаунта);

[1] Chinese Tech Companies Still Can't Stop Medical Data Leaks. – URL: https://technode.com/2020/01/09/chinese-tech-companies-still-cant-stop-medical-data-leaks/ (дата обращения: 17.03.2026).

[2] Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications. – URL: https://www.chinalawtranslate.com/en/necessary-app-info/ (дата обращения: 22.07.2026).

– данные о пользователе (пол, возраст, рост, вес, без которых нельзя рассчитать нормы калорий или индекс массы тела);

– специфические биометрические и медицинские данные с устройства (данные о частоте сердечных сокращений, шагах, уровне глюкозы, показатели ЭКГ, которые собираются напрямую с умного тонометра или фитнес-браслета для выполнения главной функции мониторинга).

Следует заметить, что многие медицинские данные относятся к «чувствительным» персональным данным согласно Закону КНР о защите личной информации. Их обработка требует еще более строгого режима: отдельного согласия в письменной форме или электронной форме, указания конкретной цели и доказательств крайней необходимости. Медицинскому работнику запрещено «связывать» предоставление услуги с согласием на избыточный сбор данных. Пациент должен быть проинформирован о конкретной цели, объеме данных, сроках хранения и третьих лицах, которым могут передаваться сведения. Любое изменение цели требует нового согласия. Тем самым Положение об объеме необходимой личной информации для общих типов мобильных приложений установило практическую основу для защиты обработки персональных данных в виде специального перечня приложений, в котором вышеуказанные требования к «чувствительной» информации распространяются в том числе на мобильные приложения из числа технологий Интернета вещей, осуществляющие сбор персональных данных пациентов.

По сравнению с Китаем, в российском законодательстве отсутствуют нормативные правовые акты, регулирующие обработку «чувствительных» персональных данных, собираемых именно приложениями из числа технологий Интернета вещей, для которых устанавливались бы дифференцированные перечни допустимого сбора; в результате нет норм по ограничению чрезмерной обработки таких данных.

В связи с этим отсутствие в России легально закрепленного исчерпывающего перечня допустимых к сбору категорий данных для конкретных типов приложений из числа технологий Интернета вещей лишает разработчиков подобных приложений и операторов обработки персональных данных четких ориентиров правомерного поведения, что создает риск избыточного сбора «чувствительных» персональных данных под видом функциональной потребности. Тем самым разработчики и операторы могут расширять спектр собираемых биометрических и медицинских данных, не имеющих

прямого отношения к диагностике или мониторингу здоровья (например геолокационные данные, сведения о социальных взаимодействиях и др.). При отсутствии отраслевого перечня типов мобильных приложений стирается грань между действительно необходимыми и второстепенными данными, что нарушает принцип минимизации, закрепленный в ч. 2 ст. 5 Федерального закона «О персональных данных», и открывает возможности для недобросовестной коммерциализации «чувствительных» персональных данных. Граждане, в свою очередь, лишены возможности оценить правомерность запрашиваемых мобильным приложением данных, что снижает прозрачность обработки.

Полагаем целесообразным принять в России аналог китайского Положения об объеме необходимой личной информации для общих типов мобильных приложений, обязывающего раскрывать минимально допустимый перечень собираемых данных применительно к категориям приложений из числа технологий Интернета вещей. Такое регулирование должно сопровождаться изданием практического руководства, в котором содержались бы критерии обоснованности сбора персональной информации. Учитывая динамику появления новых медицинских приложений и устройств, в том числе обычных мобильных приложений, не имеющих медицинского предназначения, назрела объективная потребность в создании динамического перечня таких приложений, сгруппированных по выполняемым медицинским функциям, что позволит контролирующему органу идентифицировать необходимый и достаточный состав обрабатываемых персональных данных.

Действующая редакция Федерального закона «О персональных данных» не содержит прямой нормы, предоставляющей Правительству РФ полномочие на утверждение исчерпывающего перечня необходимых данных для категорий мобильных приложений. Поэтому первым этапом должно стать внесение точечных изменений в положения указанного Федерального закона, которые создадут фундамент для будущего перечня.

Заключение

Стремительное развитие информационных технологий формирует фундаментально новую парадигму здравоохранения, основанную на персонализации лечения, предиктивной аналитике и непрерывном мониторинге состояния пациентов. Однако преимущества информационных технологий неразрывно сопряжены с

возникновением рисков в сфере частной жизни, что превращает проблему защиты персональных данных в одну из самых важных в условиях цифровизации здравоохранения.

Как в российской, так и в зарубежной практике центральным объектом защиты выступают «чувствительные» персональные данные, содержащие сведения о состоянии здоровья, генетическую и биометрическую информацию. Сопоставление европейской модели с российским законодательством выявляет общую тенденцию к установлению специальных режимов обработки таких данных, однако существующий подход становится недостаточно эффективным. В условиях автоматизированной обработки данных ИИ требуется переход к более гибкой модели регулирования, при которой уровень мер предосторожности соразмерен вероятности и серьезности потенциального вреда для субъекта данных.

Опыт КНР представляет особый интерес, демонстрируя попытки синхронизировать технологическое развитие с законодательными реформами. Принятие Закона КНР о защите личной информации и внедрение требований о минимизации сбора данных для мобильных приложений указывают на практический вектор решения проблемы утечек персональных данных. Изучение китайского подхода, в частности принципов раскрытия минимально необходимого перечня собираемых сведений и создания динамических реестров медицинских приложений, может быть эффективно использовано для совершенствования российского законодательства.

Учет передового зарубежного опыта, в том числе китайского, позволит России выстроить сбалансированную систему правовых гарантий, при которой использование инновационных информационных технологий не будет вступать в конфликт с конституционным правом на неприкосновенность частной жизни.

С появлением новых информационных технологий в будущем будут разработаны высокотехнологичные и передовые методы, которые смогут сделать конфиденциальность и безопасность медицинских данных более надежными. Это также становится новой темой исследований, поскольку практически все медицинские и другие конфиденциальные персональные данные находятся в сети или на периферийных устройствах.