DOI: 10.17803/1729-5920.2023.204.11.117-128

М. В. Некотенева
Д. В. Пономарёва
Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Развитие правового регулирования применения мобильных медицинских технологий (mHealth) в праве международных интеграционных объединений: опыт Европейского Союза

Резюме. В статье рассмотрен опыт правового регулирования применения мобильных медицинских технологий (ММТ, mHealth) в крупнейшем региональном интеграционном объединении — Европейском Союзе (ЕС). Отмечается, что цифровое здравоохранение представляет собой многогранное понятие, включающее в себя различные аспекты общественного здравоохранения и окружающую его цифровую среду. Диджитализация здравоохранения охватывает: медицинские процессы, включая программное обеспечение для поддержки работы врачей (в том числе технологии телемедицины), инструменты управления медицинским учреждением, удаленное взаимодействие с пациентами и мониторинг такого взаимодействия; аналитику больших данных для разработки лекарственных препаратов, управления клиническими исследованиями, изучения популяции больных; дополнительные инструменты, ориентированные на пациента и включающие приложения, связанные с определением физического состояния и курса лечения, а также соблюдения режима приема лекарственных препаратов. В статье представлен детальный обзор основных документов ЕС в релевантной сфере, на примере конкретных судебных дел проиллюстрировано влияние судебной практики на развитие регуляторики в области применения мобильных медицинских технологий, а также проанализированы механизмы саморегулирования в рассматриваемой сфере. Подчеркивается, что в то время как саморегулирование со стороны магазина приложений может задать разработчикам приложений для мобильного здравоохранения правильное направление путем преобразования положений Регламента 2016/679 (GDPR) в технические требования предварительного утверждения, соблюдению положений о конфиденциальности способствует повышенная осведомленность как пользователей приложений и разработчиков, так и брокеров медицинских данных о рисках для соблюдения основных прав человека со стороны приложений мобильного здравоохранения. В заключение авторами сформулированы ключевые проблемы и пути совершенствования нормативного регулирования ЕС в области применения мобильных медицинских технологий, рекомендовано использование передового опыта ЕС в развитии нормативного регулирования ММТ в Российской Федерации и интеграционных объединениях с ее участием.

Ключевые слова: мобильные медицинские технологии; электронное здравоохранение; правовое регулирование; международные интеграционные объединения; региональные международные организации; судебная практика; цифровое здравоохранение; цифровые технологии; Европейский Союз (ЕС); региональное регулирование; вторичное право; директива; регламент; источник права; саморегулирование
Для цитирования: Некотенева М. В., Пономарева Д. В. Развитие правового регулирования применения мобильных медицинских технологий (mHealth) в праве международных интеграционных объединений: опыт Европейского Союза. *Lex russica*. 2023. Т. 76. № 11. С. 117–128. DOI: 10.17803/1729-5920.2023.204.11.117-128

Благодарности. Исследование выполнено в рамках программы стратегического академического лидерства «Приоритет-2030».

Development of Legal Regulation of the Use of Mobile Medical Technologies (mHealth) in the Law of International Integration Associations: European Union Experience

Maria V. Nekoteneva
Darya V. Ponomareva
Kutafin Moscow State Law University (MSAL)
Moscow, Russian Federation

Abstract. The paper examines the experience of legal regulation of the use of mobile medical technologies (MMT, mHealth) in the largest regional integration association — the European Union (EU). It is noted that digital healthcare is a multifaceted concept that includes various aspects of public health and the digital environment surrounding it. Digitalization of healthcare covers medical processes, including software to support the work of doctors (including telemedicine technologies), tools for managing a medical institution, remote interaction with patients and monitoring such interaction; big data analytics for drug development, clinical research management, patient population studies; additional patient-oriented tools and including applications related to the determination of physical condition and the course of treatment, as well as compliance with the medication regimen. The paper provides a detailed overview of the main EU documents in the relevant field, illustrates the impact of judicial practice on the development of regulation in the field of mobile medical technologies, and analyzes the mechanisms of self-regulation in this area using the example of specific court cases. It is emphasized that while self-regulation on the part of the applications store can set developers of mobile healthcare applications in the right direction by converting the provisions of Regulation 2016/679 (GDPR) into technical requirements for preliminary approval, compliance with privacy provisions is facilitated by increased awareness of both application users and developers, as well as brokers of medical data about the risks to the observance of fundamental human rights. from the side of mobile healthcare applications. In conclusion, the authors formulated the key problems and ways to improve EU regulatory framework in the field of mobile medical technologies, recommended the use of EU best practices in the development of MMT regulatory regulation in the Russian Federation and integration associations with its participation.
Keywords: mobile medical technologies; electronic healthcare; legal regulation; international integration associations; regional international organizations; judicial practice; digital healthcare; digital technologies; European Union (EU); regional regulation; secondary law; directive; regulation; source of law; self-regulation
Cite as: Nekoteneva MV, Ponomareva DV. Development of Legal Regulation of the Use of Mobile Medical Technologies (mHealth) in the Law of International Integration Associations: European Union Experience. *Lex russica*. 2023;76(11):117-128. (In Russ.). DOI: 10.17803/1729-5920.2023.204.11.117-128

Acknowledgements. The study was carried out within the framework of «Priority-2030» Strategic Academic Leadership Program.

Введение

Цифровое здравоохранение представляет собой многогранное понятие, включающее в себя различные аспекты общественного здравоохранения и окружающую его цифровую среду. Диджитализация здравоохранения охватывает: медицинские процессы, включая программное обеспечение для поддержки работы врачей (в том числе технологии телемедицины), инструменты управления медицинским учреждением, удаленное взаимодействие с пациентами и мониторинг такого взаимодействия; аналитику больших данных для разработки лекарственных препаратов, управления клиническими исследованиями, изучения популяции больных; дополнительные инструменты, ориентированные на пациента и включающие приложения, связанные с определением физического состояния и курса лечения, а также соблюдения режима приема лекарственных препаратов[1].

К наиболее распространенным цифровым технологиям в сфере здравоохранения можно отнести:

а) 3D-печать, используемую для изготовления индивидуальных медицинских изделий (таких как импланты), а также в качестве пере-

[1] URL: https://www.simmons-simmons.com/en/publications/ckpzd2qes1c7l0968v55dor5l/digital-health-a-european-legal-framework (дата обращения: 04.06.2023).

довой технологии — для печати биологического материала;

б) дополненную виртуальную реальность для рекламы, обучения (пациентов и медицинских работников) или терапевтических целей;

в) искусственный интеллект (ИИ). Европейская комиссия определяет его как «программное обеспечение, которое разработано с использованием одного или нескольких методов и подходов <…> и которое может для заданного набора поставленных целей генерировать результаты, такие как содержание, прогнозирование, рекомендации или решения, влияющие на среду, с которой они взаимодействуют»[2]. В настоящее время ИИ используется в медицинских целях для обеспечения проведения интеллектуального анализа данных, в том числе для целей диагностики заболеваний, выявления биомаркеров, определения идеальных препаратов для проведения клинических испытаний;

г) блокчейн, который применяется как технология отслеживания при создании цепочек поставок медицинских продуктов и управления клиническими испытаниями;

д) дроны, являющиеся перспективной технологией для использования при транспортировке лекарственных средств и биологического материала, в том числе органов;

е) интернет вещей (IoT), применяемый для удаленного наблюдения и так называемой удаленной хирургии (речь идет в том числе об использовании медицинских (хирургических) роботов);

ж) программное обеспечение, в частности, мобильные приложения, которые используются для различных целей: самодиагностики, медицинского обучения пациентов (например, для самостоятельного назначения лечения или соблюдения режима лечения), содействия в проведении научных исследований (клинических исследований), помощи медицинским работникам.

В данной статье рассмотрен опыт правового регулирования применения мобильных медицинских технологий (ММТ, mHealth) в крупнейшем региональном интеграционном объединении — Европейском Союзе (ЕС).

Источники вторичного права в сфере мобильного медицинского здравоохранения (mHealth)

Применительно к Европейскому Союзу как эффективно функционирующему на европейском пространстве интеграционному объединению сто́ит подчеркнуть, что в его пределах создана единая правовая среда в области цифрового, в том числе мобильного, здравоохранения. Нормативную основу в указанной сфере составляют следующие документы Союза:

а) Регламент Европейского парламента и Совета Европейского Союза 2017/745 от 05.04.2017 о медицинских изделиях, об изменении Директивы 2001/83/ЕС, Регламента (ЕС) 178/2002 и Регламента (ЕС) 1223/2009, а также об отмене Директив 90/385/ЕЭС и 93/42/ЕЭС Совета ЕС;

б) Регламент Европейского парламента и Совета Европейского Союза 2017/746 от 05.04.2017 о медицинских изделиях для диагностики in vitro, а также об отмене Директивы 98/79/ЕС и Решения 2010/227/ЕС Европейской Комиссии;

в) Директива Европейского парламента и Совета Европейского Союза 2006/42/ЕС от 17.05.2006 о машинах и механизмах;

г) Регламент Европейского парламента и Совета Европейского Союза 1025/2012 от 25.10.2012 о европейской стандартизации, изменении Директив 89/686/ЕЭС и 93/15/ЕЭС Совета ЕС и Директив 94/9/ЕС, 94/25/ЕС, 95/16/ЕС, 97/23/ЕС, 98/34/ЕС, 2004/22/ЕС, 2007/23/ЕС, 2009/23/ЕС и 2009/105/ЕС Европейского парламента и Совета ЕС и отмене Решения 87/95/ЕЭС Совета ЕС и Решения 1673/2006/ЕС Европейского парламента и Совета ЕС;

д) Директива Совета Европейских Сообществ 2013/59/Евратом от 05.12.2013, устанавливающая базовые стандарты защиты от рисков, возникающих от воздействия ионизирующего излучения, и отменяющая Директивы 89/618/Евратом, 90/641/Евратом, 96/29/Евратом, 97/43/Евратом и 2003/122/Евратом;

е) Директива Европейского парламента и Совета Европейского Союза 2005/36/ЕС от 07.09.2005 о признании профессиональных квалификаций;

ж) Директива Европейского парламента и Совета Европейского Союза 2011/24/ЕС от 09.03.2011 о правах пациентов в трансграничном медицинском обслуживании;

[2] См.: Предложение Европейской Комиссии о Регламенте об искусственном интеллекте — Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence

з) Директива Совета Европейских Сообществ от 25.07.1985 № 85/374/ЕЭС о сближении законов, регламентов и административных положений государств-членов, применяемых к ответственности за неисправную продукцию;

и) Директива 2001/95/ЕС Европейского парламента и Совета от 03.12.2001 об общей безопасности продукции;

к) Директива Европейского парламента и Совета ЕС (ЕС) 2016/1148 от 06.07.2016 о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза;

л) Регламент Европейского парламента и Совета 2019/1020 от 20.06.2019 о надзоре за рынком и соблюдении требований к продуктам и вносящий поправки в Директиву 2004/42/ЕС и Регламенты (ЕС) № 765/2008 и (ЕС) № 305/2011;

м) Регламент Европейского парламента и Совета Европейского Союза 2016/679 от 27.04.2016 о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных — General Data Protection Regulation / GDPR);

н) Директива Европейского парламента и Совета Европейского Союза 96/9/ЕС от 11.03.1996 о правовой охране баз данных;

о) Директива Европейского парламента и Совета Европейского Союза 2016/943 от 08.06.2016 о защите конфиденциальных ноу-хау и деловой информации (коммерческой тайны) от незаконного приобретения, использования и раскрытия;

п) Директива Европейского парламента и Совета Европейского Союза 2019/790 от 17.04.2019 об авторском праве и смежных правах на едином цифровом рынке, а также об изменении Директив 96/9/ЕС и 2001/29/ЕС.

Применение Регламентов 2017/745 и 2017/746 необходимо для квалификации и классификации медицинских технологий, определения того, является ли технология медицинским устройством (в том числе для диагностики in vitro). Квалификация технологии как медицинского устройства по нормам права ЕС предполагает нанесение соответствующей маркировки; определяет, каковы обязательства операторов, участвующих в производстве и распространении указанных устройств, а также каковы направления и способы использования таких технологий. Требования к техническим характеристикам новейших медицинских устройств содержатся в Директиве 2006/42/ЕС, Регламенте 1025/2012, Директиве 2013/59/Евратом. Директивы 2005/36/ЕС и 2011/24/ЕС применяются также в контексте телемедицины, хотя здесь всё же остается достаточно высокой роль национального законодателя.

Что касается вопросов обеспечения контроля ответственности и рисков в рассматриваемой сфере, то здесь сто́ит назвать Директиву 85/374/ЕЭС (предусматривает ответственность за продукты с дефектами), Директиву 2001/95/ЕМ (включает положения об обеспечении общей безопасности продукции), Директиву 2016/1148 (содержит меры по обеспечению высокого общего уровня безопасности сетевых и информационных систем в Союзе), а также Регламент 2019/1020 (положения данного Регламента применяются к медицинским устройствам как lex generalis).

Безусловно, важнейшим аспектом цифрового здравоохранения, в том числе применения мобильных медицинских технологий, является защита и обеспечение конфиденциальности персональных данных пациентов (в качестве основного документа применяется Регламент 2016/679 (GDPR)). Ключевое значение также имеют документы, предусматривающие охрану прав интеллектуальной собственности, созданной с использованием указанных данных: Бернская конвенция об охране литературных и художественных произведений 1886 г., Европейская патентная конвенция 1973 г., Директива 96/9/ЕС (посвящена правовой охране баз данных), Директива 2016/943 (регламентирует защиту коммерческой тайны) и Директива 2019/790 (предусматривает защиту авторских и смежных прав в пределах Единого цифрового рынка).

Таким образом, для регулирования деятельности, связанной с цифровым и мобильным здравоохранением, в ЕС сформирована согласованная, хотя и фрагментированная правовая база.

При этом выше перечислены документы, которые содержат общеевропейские правила в отношении цифровых технологий в области здравоохранения. Есть ряд существенных вопросов, которые в нормативном разрезе могут

(Artificial Intelligence Act) and Amending Certain Union Legislative Acts, COM/2021/206 final // URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 (дата обращения: 04.06.2023).

быть разрешены только на уровне отдельных государств, поскольку те или иные правила не могут быть гармонизированы в силу различных причин. К таким вопросам относятся: налоговое регулирование (налоговые правила необходимо определить в соответствии с национальным законодательством, например, в случае предоставления медицинских услуг онлайн); возмещение расходов на разработку и внедрение новых медицинских технологий (данный вопрос остается сугубо национальной прерогативой); гражданско-правовая и уголовная ответственность за нарушение требований к качеству продукции.

Помимо развития собственного наднационального регулирования, ЕС активно сотрудничает с ВОЗ, учредив партнерство в области цифрового здравоохранения[3]. Дополнительным стимулом для развития сотрудничества крупнейшего европейского интеграционного объединения и единственной глобальной международной организации в области здравоохранения послужила пандемия COVID-19, распространение которой побудило государства обеспечить глобальную мобильность и защиту граждан от угроз здоровью. Партнерство ВОЗ-ЕС является инициативным структурным элементом Глобальной сети цифровой сертификации здоровья ВОЗ, которая будет разрабатывать широкий спектр цифровых продуктов для улучшения здоровья населения. Такое сотрудничество основано на общих ценностях и принципах прозрачности, открытости, инклюзивности, подотчетности, защиты данных, конфиденциальности, безопасности, масштабируемости на глобальном уровне.

Сотрудничество ВОЗ и ЕС в области цифрового здравоохранения распространяется и на разработку мобильных медицинских приложений. Всё большее число граждан Евросоюза используют мобильные приложения для самоконтроля здоровья[4]. Обработка больших данных о здоровье человека с помощью программного обеспечения, используемого в приложениях, создает серьезные риски для личной автономии пользователей таких приложений. Эти риски усугубляются отсутствием на уровне ЕС специального правового регулирования в области мобильного здравоохранения и неприменимостью к указанной области правовой базы ЕС в отношении здоровья и прав пациентов. Хотя Регламент 2016/679 (GDPR) предусматривает прочную нормативную основу для защиты данных о здоровье пациента, на практике многие положения локальных документов, на основании которых разрабатываются и используются приложения mHealth, не соответствуют европейским требованиям.

Ключевые риски связаны с обработкой больших объемов данных о состоянии здоровья и с возможностями передачи данных третьим лицам. Не сто́ит забывать, что пользователи обладают ограниченной информацией и осуществляют лимитированный контроль над тем, кто́ имеет доступ к информации об их здоровье[5]. Возникает парадоксальная ситуация: пользователи применяют мобильные приложения, чтобы расширить возможности для улучшения собственного здоровья, при этом контроль за данными о собственном здоровье они не осуществляют[6].

Указанные риски обостряются в связи с тем, что на уровне ЕС отсутствует эффективное (не фрагментарное) правовое регулирование обозначенной сферы. Правовая база ЕС, представленная выше, не распространяется на пользователей приложений mHealth для самоконтроля здоровья. Когда традиционное нормативное регулирование не приводит к ожидаемому результату, на помощь приходят альтернативные формы и способы регулирования. В целях обеспечения защиты данных о здоровье пациентов в рамках мобильных приложений онлайн-платформы распространения мобильных приложений (магазины приложений) могут применять инструменты саморегулирования. Магазины приложений в ЕС предлагают упорядоченное, иерархическое регулирование применения мобильных медицинских приложений, обеспечивая процедуру их проверки. Магазины требуют от разработчиков приложений соблюдать определенные правила в рамках процесса

[3] URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3043 (дата обращения: 04.06.2023).

[4] *Incisive Health International,* Taking the Pulse of eHealth in the EU: An Analysis of Public Attitudes to eHealth Issues in Austria, Bulgaria, Estonia, France, Germany, Italy, and the UK (2017).

[5] *Spiller K.* et al. Data Privacy: Users' Thoughts on Quantified Self Personal Data // Self-Tracking: Empirical and Philosophical Investigations / Btihaj Ajana ed. 2018. P. 111–124.

[6] *Lucivero F., Jongsma K. R.* A Mobile Revolution for Healthcare? Setting the Agenda for Bioethics // J. Med. Ethics. 2018. 44. P. 685.

утверждения цифрового продукта, в том числе удаление приложения, если оно не соответствует требованиям. Подобная форма отраслевого саморегулирования позволяет магазинам приложений влиять на разработчиков.

К популярным мобильным приложениям в сфере здравоохранения относятся счетчики калорий, приложения для контроля менструального цикла и беговые трекеры. Такие приложения отслеживают поведение пользователей в течение длительного времени. Приложения mHealth нацелены в первую очередь на помощь в поддержании физической формы и в целом здорового образа жизни, поэтому они аккумулируют большие объемы сведений, связанных со здоровьем, в том числе биометрические данные, информацию о жизненно важных функциях организма и ключевые показатели здоровья. Согласно Регламенту 2016/679 (GDPR) речь идет о «данных о здоровье» в широком смысле. Определение данных о здоровье предполагает, например, и то, что информация об употреблении алкоголя за определенный период также рассматривается как сведения о здоровье, поскольку она связана с рисками возникновения определенных заболеваний. Тем не менее некоторые сведения не являются изначально данными о состоянии здоровья, но могут трансформироваться в таковые при проведении мониторинга в течение длительного времени (например, среднее количество шагов в месяц, измеряемое при помощи приложения-шагомера), также сведения о здоровье могут объединяться с другими данными (в частности, сведениями о ежедневном употреблении калорий, информацией в профиле в социальных сетях)[7].

Вероятность нарушения прав пользователей мобильных медицинских приложений, в частности конфиденциальности информации, весьма высока. Неправильное использование данных о здоровье может привести к необратимым последствиям для субъектов данных и общественной среды. Очевидно, что такие данные представляют собой ценный товар, и компании, вовлеченные в работу с big data, проявляют к ним повышенный интерес вследствие дорогостоящего процесса их сбора[8]. Мобильное приложение может стимулировать пользователей предоставлять всё больше данных о состоянии их здоровья, ведь это может гарантировать ему бóльшую прибыль. В приложениях аккумулируются так называемые пассивно собираемые данные, например обзоры среднего количества шагов за месяц, которые регулярно сохраняются вне контроля пользователей. Кроме того, мобильные приложения для здоровья части применяют стандартные условия использования, действующие по принципу «прими или откажись» (англ. take it or leave it). Таким образом, пользователи не всегда осознают точный объем и тип собираемых данных[9].

Существуют разумные опасения в отношении контроля пользователя над доступом к собранным данным о состоянии его здоровья. Большинство приложений предусматривают возможность раскрытия информации в будущем неопределенной аудитории. Так, многие приложения mHealth обмениваются данными о состоянии здоровья между анонимными пользователями в целях сопоставления, операторы приложений могут продавать данные о здоровье третьим лицам (рекламодателям, страховым компаниям, банковским организациям и т.д.). Приложения часто не позволяют детализировать согласие на обработку персональных данных: пользователи вынуждены давать согласие в отношении всех получателей и типов данных. Необходимо подчеркнуть, что обработка больших данных о состоянии здоровья и обмен ими с третьими лицами в рамках приложений mHealth компрометируют пользователей и могут представлять угрозу их праву на неприкосновенность частной жизни.

В ЕС вопросы конфиденциальности информации о здоровье регулируются разветвленной системой нормативных актов, частично названных выше. На национальном уровне неприкосновенность частной жизни гарантируется системой защиты прав пациентов. Принцип конфиденциальности медицинской информации красной нитью проходит через релевантное национальное правовое регулирование. Конфиденциальность медицинской информации подразумевает право пациента на конфиденциальность личных данных, а также обязанность медицинских работников защищать данные от несанкционированного доступа. Вместе с тем пользователи приложений mHealth, как правило, не считаются пациентами ни с точки

[7] Art. 29 Data Protection Working Party, Annex — health data in apps and devices (2015).

[8] *Cecere G.* et al. Economics of Free Mobile Applications: Personal Data as a Monetization Strategy. 2018. P. 45.

[9] *Ostherr K.* et al. Trust and Privacy in the Context of User-Generated Health Data // Big data & Soc'y. 2017. 4.

зрения разработчиков приложений, ни с позиции действующей регуляторики, поскольку приложения не служат собственно медицинским целям и в их работе не участвует медицинский персонал. Таким образом, пользователи приложений не подпадают под систему защиты прав пациентов[10].

На уровне Европейского Союза применение мобильных медицинских технологий охватывается регулированием медицинских устройств в соответствии с Регламентом 2017/745. Под действие указанного документа подпадает также программное обеспечение (включая мобильные приложения), но только такое, которое разработано для целей, обозначенных в Регламенте 2017/745. Поскольку большинство мобильных приложений для самоконтроля состояния здоровья (мониторинг физической формы, общего состояния здоровья) не предназначены для целей медицины (лечения), а сосредоточены лишь на общем состоянии здоровья, они не рассматриваются как медицинские устройства и не подпадают под действие названного Регламента. Впрочем, если приложение mHealth имеет предполагаемое медицинское назначение (это могут быть приложения для самоконтроля, рекомендованные врачом), Регламент 2017/745 может быть применен. В любом случае, данный Регламент обеспечивает защиту конфиденциальности информации о здоровье в соответствии с Регламентом 2016/679 (GDPR).

Регламент 2016/679 (GDPR) является основным инструментом защиты конфиденциальности данных о здоровье в Европейском Союзе и применяется к приложениям mHealth, доступным для использования в ЕС. Основной принцип, заложенный в Регламент 2016/679 (GDPR), гласит: любая обработка персональных данных должна осуществляться на основании закона. Регламент предусматривает обязанности обработчиков и контролеров обработки данных, а также предоставляет права субъектам данных для усиления контрольных полномочий с их стороны. Документом закрепляется специальный режим защиты данных о здоровье, который предполагает общий запрет на обработку данных о состоянии здоровья, но предусматривает ограниченные отступления в том случае, если данные о состоянии здоровья представляют общественный интерес и не связаны с профессиональной тайной. В рамках приложения mHealth данные о состоянии здоровья подлежат обработке только в том случае, если пользователи предоставят явно выраженное согласие. Регламент 2016/679 (GDPR) установил максимально широкую защиту конфиденциальности персональных данных в сочетании со строго регламентированными правилами обработки и передачи таких данных, что в значительной степени способствует эффективной защите прав пользователей приложений mHealth.

Тем не менее важно обратить внимание на то, что ряд эмпирических исследований демонстрируют фактическое несоответствие многих приложений положениям Регламента 2016/679 (GDPR)[11]. В частности, согласно исследованию около 20 мобильных медицинских приложений не соблюдают требование об обязательном согласии пользователя на обработку персональных данных: бóльшая часть приложений (около 55 %) предоставляют информацию о политике конфиденциальности только перед регистрацией пользователя, лишь 5 % приложений запрашивают согласие каждый раз, когда пользователь делится дополнительной информацией личного характера, ни одно из приложений не предполагает применения явно выраженного согласия с помощью заполнения формы-анкеты (онлайн-формы), 35 % приложений предлагают возможность отзы́ва согласия и удаления данных о состоянии здоровья[12]. В другом исследовании было отмечено, что из 24 проанализированных приложений mHealth 79 % отправляют данные о состоянии здоровья пользователя третьим лицам непрозрачным способом[13].

Таким образом, на практике довольно большое число мобильных медицинских приложений, применяемых в ЕС, не соответствуют требованиям Регламента 2016/679 (GDPR). Это

[10] Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document Green Paper on mobile Health («mHealth») (2014).

[11] *Grundy Q.* et al. Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis // BMJ. 2019. 364. l920.

[12] *Papageorgiou A.* et al. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice/ PP IEEE Access 1–1 (2018).

[13] *Grundy Q.* et al. Op. cit.

объясняется тем, что приложения разрабатываются людьми, которые не компетентны в вопросах применения европейского наднационального законодательства о защите персональных данных. Вследствие большого числа доступных приложений надзор со стороны регулирующих органов весьма затруднен из-за нехватки соответствующих ресурсов. В большинстве государств — членов ЕС отсутствуют организации, отвечающие за нормативный надзор за применением приложений mHealth. Отсутствие надзора приводит к снижению уровня соблюдаемости требований. Регламент 2016/679 (GDPR) предлагает актуальную и достаточную правовую основу для обеспечения защиты данных о состоянии здоровья, но игнорирование разработчиками приложений его требований делает указанный документ неэффективным.

Отсутствие эффективного законодательного регулирования приводит к необходимости поиска альтернативной регуляторики, коей в данном случае вполне может стать саморегулирование. Не умаляя значимости магазинов приложений в обеспечении соответствия мобильных продуктов требованиям Регламента 2016/679 (GDPR) и роли цифровых платформ в защите основных прав пользователей, центральный вопрос относительно применения данных приложений следует связать с социальными проблемами медиаплатформ.

Саморегулирование можно определить как «процесс регулирования, посредством которого организация на уровне отрасли, а не на уровне органов государственной власти или организации… устанавливает и обеспечивает соблюдение правил и стандартов, касающихся поведения организаций в отрасли»[14]. К преимуществам саморегулирования относятся гибкость в адаптации правил к технологическим изменениям, более высокое качество правил и приверженность субъектов саморегулирования им. Тем не менее саморегулирование имеет и свои ограничения, особенно применительно к защите основных прав. Инструменты саморегулирования далеко не всегда предполагают наличие действующих механизмов правоприменения и мониторинга. В отдельных случаях инструменты саморегулирования не согласуются с другими существующими нормами, что делает общую систему регулирования всё более сложной.

В контексте обеспечения защиты данных саморегулирование становится распространенным явлением. Компании предпочитают дополнять действующее законодательство инструментами саморегулирования вследствие необходимости обеспечить защиту прав потребителей, повысить общественное доверие и репутацию, ликвидировать негативное общественное мнение. Регламент 2016/679 (GDPR) поддерживает и поощряет саморегулирование предприятий в форме кодексов поведения и обязательных корпоративных правил. Кроме того, Европейская комиссия предприняла (пока, правда, безуспешно) шаги по созданию добровольного Кодекса поведения в отношении конфиденциальности данных в рамках приложений мобильного здравоохранения для разработчиков[15].

В отраслевом саморегулировании в области mHealth заметно, что магазины приложений уже играют важную роль, регламентируя в том числе сторонние приложения mHealth, распространяемые на их платформах. Такая экосистема работает следующим образом: разработчику необходимо разместить свой продукт в магазине приложений, чтобы широкий круг потребителей могли загрузить его на свои мобильные устройства; магазины приложений требуют от разработчиков соблюдать определенные правила в рамках процесса предварительного утверждения и могут удалять не соответствующие требованиям права ЕС приложения.

Функционирование магазинов приложений не охватывается Регламентом 2016/679 (GDPR). Магазины не рассматриваются правом ЕС как обработчики или контролеры данных, поскольку они не осуществляют контроль над личными данными пользователей, а просто предоставляют поставщикам приложений платформу, на которой те могут размещать цифровые продукты. Однако магазины приложений могут влиять на то, как сторонние приложения, которые квалифицируются как обработчики данных, обеспечивают защиту таких данных. Именно

[14] *Gupta A. K.*, *Lad L. J.* Industry Self-Regulation: An Economic, Organizational, and Political Analysis // AMR. 1983. 8. P. 416.

[15] European Commission, Guidance Document Medical Devices — Scope, Field of Application, Definition — Qualification and Classification of Stand Alone Software (2016).

поэтому магазины приложений применяют форму отраслевого саморегулирования. Хотя магазины приложений применяют эти правила к сторонним приложениям добровольно, саморегулирование не является добровольным с точки зрения разработчиков приложений.

Рассмотрим примеры того, как действия магазинов приложений в отношении конфиденциальности данных влияют на эффективность методов защиты данных о здоровье пользователя.

Судебная практика, повлиявшая на формирование подходов Европейского Союза к правовому регулированию применения мобильных медицинских технологий

Кейс Apple Store. Для того чтобы разработчики могли размещать приложения в Apple App Store, они должны зарегистрироваться в программе Apple Developer Program, на которую распространяет действие соответствующее лицензионное соглашение. Кроме того, Apple App Store проверяет все размещаемые приложения и обновления приложений согласно руководству по проверке App Store[16]. Данное руководство содержит особые правила для приложений mHealth — они могут подвергаться более тщательной проверке. Руководство также содержит следующие общие положения об обработке персональных данных и о конфиденциальности:

а) приложения должны предусматривать политику конфиденциальности, объясняющую, ка́к пользователи могут осуществлять свои права на сохранение, удаление и отзы́в согласия;

б) сбор данных должен основываться на согласии пользователя, пользователям должна быть предоставлена доступная и понятная возможность отозвать согласие;

в) приложения должны свести к минимуму сбор данных; при обмене данными с третьими лицами необходимо согласие пользователя;

г) приложения не должны пытаться создать профиль пользователя на основе собранных данных;

д) разработчики приложений должны учитывать конфиденциальность данных пользователя и соблюдать соответствующее законодательство о конфиденциальности.

Руководство содержит четкие правила в отношении данных о состоянии здоровья, обрабатываемых приложениями mHealth. Предусматривается, что приложения не могут использовать или раскрывать собранные данные о состоянии здоровья третьим лицам в целях рекламы, маркетинга или майнинга; не могут использовать данные о здоровье для целевой или поведенческой рекламы. Тем не менее приложения mHealth могут применять или раскрывать данные о здоровье в целях улучшения управления здоровьем и проведения исследований в области здравоохранения, но только с разрешения пользователя. В руководстве отмечается, что разработчики не могут вводить неточные данные в приложения mHealth, а сами приложения не могут сохранять информацию о состоянии здоровья в облачном хранилище iCloud.

Кейс Google Play. Критерии проверки приложений для Google Play изложены в дистрибьюторском соглашении для разработчиков и программной политике для разработчиков[17]. Дистрибьюторское соглашение действует как юридически обязывающий договор между разработчиком приложения и компанией Google. Что касается обработки персональных данных, то в соглашении говорится, что приложения должны соответствовать применимым нормам о защите данных, в частности, информировать пользователей о том, какие личные данные подлежат обработке, предоставлять уведомление о конфиденциальности и обеспечивать надлежащую защиту данных. Кроме того, приложения могут использовать персональные данные только в тех целях, на которые дал согласие пользователь.

Программная политика для разработчиков содержит дополнительные рекомендации по обработке персональных данных о состоянии здоровья. Так, строго запрещены приложения, предназначенные для злоупотребления или неправомерного использования персональных данных. Кроме того, функционирование приложения должны быть прозрачным в отношении сбора, использования и обмена персональными данными. Что касается конфиденциальных персональных данных, которые включают также данные о состоянии здоровья, в политике указано, что сбор и использование

[16] *Apple App Store,* App Store Review Guidelines (2019) // URL: https://developer.apple.com/app-store/review/guidelines/ (дата обращения: 04.06.2023).

[17] Google Play, Google Play Developer Distribution Agreement (Nov. 5, 2019).

должны быть ограничены целями, непосредственно связанными с функциональностью приложения. При этом политика конфиденциальности должна быть опубликована в самом приложении. Раскрытие информации в приложении должно содержать запрос согласия пользователя до обработки данных, требующий подтверждения действий пользователя. В таких запросах на разрешение должны быть четко указаны цели обработки или передачи данных. Кроме того, подчеркивается, что персональные данные могут использоваться только в целях, на которые дал согласие пользователь.

Анализ указанных кейсов позволяет сделать вывод о том, что магазины приложений действительно обеспокоены вопросами обеспечения конфиденциальности. Тем не менее такая обеспокоенность не гарантирует более высокий уровень защиты персональных данных пользователей приложений mHealth. В документах обоих магазинов приложений отмечается, что приложения должны соответствовать законодательству о конфиденциальности и интегрировать политику конфиденциальности. Вместе с тем уровень детализации положений о конфиденциальности соответствующих магазинов приложений значительно различается. В то время как документация Apple App Store ретранслирует большинство принципов защиты данных и прав субъектов данных, отраженных в Регламенте 2016/679 (GDPR), правила конфиденциальности Google Play сформулированы несколько расплывчато и не упоминают права субъектов данных. Таким образом, документы Google Play не предлагают разработчикам приложений необходимые рекомендации о том, как защитить личные данные, особенно в отношении прав субъектов данных. Это влечет за собой большой риск того, что права пользователей просто попадут в политику конфиденциальности приложения мелким шрифтом и не приведут к эффективной защите конфиденциальности персональных данных.

Заключение

Как это ни парадоксально, желание людей расширить свои возможности с помощью приложений мобильного здравоохранения приводит к тому, что пользователи теряют возможность контролировать обработку данных о собственном здоровье. Хотя теоретически Регламент 2016/679 (GDPR) предлагает надежное решение для защиты данных о здоровье пользователей приложений mHealth, на практике ему не хватает должной эффективности. Инструменты саморегулирования, используемые магазинами приложений, могут заполнить пробел в регуляторике и тем самым способствовать повышению уровня защиты данных о состоянии здоровья в ЕС. Данный тезис подтверждает мысль о том, что Европейский Союз всё активнее вовлекается в регулирование применения цифровых технологий и связанных с ними рисков нарушения основополагающих прав человека. Союз в своей деятельности продвигает и поддерживает структуры саморегулирования в дополнение к релевантным нормативным актам, принимаемым на уровне ЕС.

Несмотря на важную роль магазинов приложений в достижении этой цели, ответственность за обеспечение защиты конфиденциальности данных о здоровье пользователей лежит на разработчиках и поставщиках приложений mHealth, которые обрабатывают медицинские данные. Приложения mHealth должны предоставлять пользователям адекватные средства для реализации прав на защиту конфиденциальности, предусматривая конкретные эффективные возможности контроля над решениями, касающимися обработки данных о состоянии здоровья. В этой связи решающее значение приобретает фактическое применение стандартов саморегулирования. В то время как саморегулирование со стороны магазина приложений может направить разработчиков приложений для мобильного здравоохранения в правильном направлении путем преобразования положений Регламента 2016/679 (GDPR) в технические требования предварительного утверждения, соблюдению соответствующих положений о конфиденциальности способствует повышенная осведомленность как пользователей приложений, разработчиков, так и брокеров медицинских данных о рисках для соблюдения основных прав человека со стороны приложений мобильного здравоохранения. Европейский Союз смог бы сыграть центральную роль в достижении этой цели, чтобы помочь пользователям приложений mHealth достичь желаемого расширения возможностей, отразив нормы и принципы Регламента 2016/679 (GDPR) в конкретных приложениях мобильного здравоохранения. Проанализированный опыт Европейского Союза в рассматриваемой области может оказаться полезным в части развития соответствующего регулирования на уровне Российской Федерации и интеграционных объединений с ее участием.

СПИСОК ЛИТЕРАТУРЫ

Cecere G. et al. Economics of Free Mobile Applications: Personal Data as a Monetization Strategy. 2018.

Grundy Q. et al. Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis // BMJ. 2019. 364. l920.

Gupta A. K., *Lad L. J.* Industry Self-Regulation: An Economic, Organizational, and Political Analysis // AMR. 1983. 8. P. 416–425.

Lucivero F., *Jongsma K. R.* A Mobile Revolution for Healthcare? Setting the Agenda for Bioethics // J. Med. Ethics. 2018. 44. P. 685–689.

Ostherr K. et al. Trust and Privacy in the Context of User-Generated Health Data // Big data & Soc'y. 2017. 4.

Papageorgiou A. et al. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice/ PP IEEE Access 1–1 (2018).

Spiller K. et al. Data Privacy: Users' Thoughts on Quantified Self Personal Data // Self-Tracking: Empirical and Philosophical Investigations / Btihaj Ajana ed. 2018. P. 111–124.

REFERENCES

Cecere G, et al. Economics of Free Mobile Applications: Personal Data as a Monetization Strategy. 2018.

Grundy Q, et al. Data Sharing Practices of Medicines Related Apps and the Mobile Ecosystem: Traffic, Content, and Network Analysis. *BMJ*. 2019;364:l920.

Gupta AK, Lad LJ. Industry Self-Regulation: An Economic, Organizational, and Political Analysis. *AMR*. 1983;8:416-425.

Lucivero F, Jongsma KR. A Mobile Revolution for Healthcare? Setting the Agenda for Bioethics. *J. Med. Ethics*. 2018;44:685-689.

Ostherr K, et al., Trust and Privacy in the Context of User-Generated Health Data. *Big data & Soc'y*. 2017;4.

Papageorgiou A, et al., Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. PP IEEE Access 1-1 (2018).

Spiller K, et al. Data Privacy: Users' Thoughts on Quantified Self Personal Data. In: Btihaj Ajana, editor. Self-Tracking: Empirical and Philosophical Investigations. 2018. Pp. 111–124.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Некотенева Мария Владимировна, кандидат юридических наук, доцент кафедры интеграционного и европейского права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация
mvnekoteneva@msal.ru

Пономарёва Дарья Владимировна, кандидат юридических наук, доцент кафедры практической юриспруденции Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация
dvponomareva@msal.ru

INFORMATION ABOUT THE AUTHORS

Maria V. Nekoteneva, Cand. Sci. (Law), Associate Professor, Department of Integration and European Law,
Kutafin Moscow State Law University (MSAL)
9, Sadovaya-Kudrinskaya St., Moscow 125993, Russian Federation
mvnekoteneva@msal.ru

Darya V. Ponomareva, Cand. Sci. (Law), Associate Professor, Department of Practical Law,
Kutafin Moscow State Law University (MSAL)
9, Sadovaya-Kudrinskaya St., Moscow 125993, Russian Federation
dvponomareva@msal.ru

Материал поступил в редакцию 21 июля 2023 г.
Статья получена после рецензирования 23 июля 2023 г.
Принята к печати 17 октября 2023 г.

Received 21.07.2023.
Revised 23.07.2023.
Accepted 17.10.2023.