Защита персональных данных в телемедицине[1]

М.С. Журавлев

младший научный сотрудник Международной лаборатории по праву информационных технологий и интеллектуальной собственности Национального исследовательского университета «Высшая школа экономики». Адрес: 101000, Российская Федерация, Москва, Мясницкая ул., д. 20. E-mail: mzhuravlev@hse.ru

Аннотация

Актуальность вопросов защиты персональных данных в телемедицине предопределена стремительным развитием информационных технологий в разных сферах общественных отношений, в том числе в сфере здравоохранения. Ключевая проблема заключается в том, что существующее правовое регулирование в области защиты персональных данных в недостаточной степени соответствует потребностям развития телемедицины. Вместо того, чтобы способствовать технологическому развитию, законодательство создает необоснованные барьеры для внедрения инноваций в здравоохранение. Эффективное функционирование современных информационно-коммуникационных технологий нуждается в обеспечении свободного, безопасного и легитимного обмена информацией между всеми субъектами телемедицинских отношений. Статья содержит рекомендации по совершенствованию законодательства о персональных данных в условиях развития телемедицины. В частности, предлагается устранить обязательное требование к письменному согласию на обработку специальных категорий персональных данных; законодательно установить специальные основания для обработки персональных данных в телемедицинских целях; дифференцировать возможность обработки персональных данных в телемедицинских целях по трем основаниям («без согласия», «без согласия, но с возможностью отказа от обработки», «с согласия»). Необходимо закрепить правовой статус субъектов телемедицинской деятельности и при необходимости предусмотреть специальные требования к обработке персональных данных этими субъектами. Кроме того, важно установить отраслевые стандарты обеспечения безопасности информационных систем здравоохранения с учетом специфичных угроз, характерных для телемедицинских технологий. Помимо требований к обработке персональных данных, в статье уделяется внимание законодательному подходу к организации информационных систем здравоохранения, без которых невозможно функционирование телемедицины. Раскрывается тезис, что законодательство в данной сфере должно способствовать интеграции и взаимодействию информационных систем здравоохранения, увеличению области полезного использования данных систем, а также повышению роли пациента в управлении персональными электронными записями о здоровье. Методологическую основу исследования составляют анализ нормативно-правовых актов и законопроектов, сравнительно-правовой метод (российский опыт сравнивается с опытом ЕС и США) и метод правового моделирования (предлагаются поправки в российское законодательство).

Ключевые слова

телемедицина, электронное здравоохранение, персональные данные, информационная безопасность, информационные системы здравоохранения, Интернет вещей, Большие данные.

Библиографическое описание: Журавлев М.С. Защита персональных данных в телемедицине // Право. Журнал Высшей школы экономики. 2016. № 3. С. 72–84.

JEL: K3; УДК: 349 DOI: 10.17323/2072-8166.2016.3.72.84

[1] Статья подготовлена в ходе работы в рамках Программы фундаментальных исследований Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ) и с использованием средств субсидии в рамках государственной поддержки ведущих университетов Российской Федерации «5-100».

Развитие информационно-коммуникационных технологий в медицине влечет за собой целый комплекс правовых вопросов[2], от решения которых зависят темпы практического внедрения достижений телемедицины, а также защита прав и законных интересов субъектов телемедицинских отношений. Одна из важных проблем развития телемедицины состоит в обеспечении свободного, безопасного и легитимного обмена информацией о состоянии здоровья граждан. Юридический аспект данной проблемы заключается в двух ключевых задачах: изменение законодательных требований к организации информационных систем здравоохранения и совершенствование правового режима персональных данных с учетом особенностей телемедицинских технологий. Обе задачи нуждаются в системном и согласованном решении.

Подходы к организации информационных систем здравоохранения подвергаются реформированию во всех странах, озабоченных вопросами распространения электронной медицины[3]. Основными тенденциями развития законодательства в этой сфере можно назвать юридическое закрепление статуса электронных записей о здоровье (*EHR — electronic health records*), обеспечение централизации этих записей и расширение прав пациентов по управлению своими записями о здоровье[4].

Действующий российский подход к информационным системам здравоохранения характеризуется недостаточной ориентированностью на использование современных информационно-коммуникационных технологий в медицине. Несмотря на то, что ст. 91 ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[5] закрепляет статус информационных систем в сфере здравоохранения, на практике функционируют системы (преимущественно в области обязательного медицинского страхования в соответствии с законом об ОМС[6]), которые в своей совокупности и по своим характеристикам не в полной мере отвечают потребностям телемедицины.

Для формирования современных централизованных систем здравоохранения в РФ действующее нормативное регулирование нуждается в совершенствовании с учетом целого ряда факторов. Во-первых, важно обеспечить дальнейшую интеграцию и взаимодействие информационных систем. На сегодняшний день российским законодательством отчасти урегулировано лишь взаимодействие операторов информационных

---

[2] В российской научной литературе правовые аспекты телемедицины освещались в следующих работах: *Наумов В.Б., Савельев Д.А.* Правовые аспекты телемедицины. СПб.: Анатолия, 2002. 107 с.; *Богдановская И.Ю.* Правовое регулирование телемедицины: опыт США // Врач и информационные технологии. 2007. № 3. С. 64–68; *Штыкова Н.Н.* Сущность и проблемы реализации электронной медицины (на примере Владимирской области) // Медицинское право. 2014. № 5. С. 22–27.

[3] Например, в Великобритании с 2002 года в рамках общей национальной программы в сфере IT (National Program for IT) разрабатывается система электронной обработки персональной информации о здоровье. Первым шагом стало создание системы записей резюме (Summary Care Records), представляющих собой электронные записи ключевой информации о здоровье пациентов. Задача создания данной системы заключается в обеспечении быстрого доступа медицинского персонала к необходимой информации о здоровье пациента в любое время и в любом месте, а также в предоставлении более удобного доступа граждан к информации о собственном здоровье. Подробнее см. http://systems.digital.nhs.uk/scr (дата обращения: 16.08.2016).

[4] См. *Carlisle G., Whitehouse D., Duquenoy P.* (Eds.). eHealth: Legal, Ethical and Governance Challenges. Springer, 2013. P. 40.

[5] Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // СЗ РФ. 2011. № 48. Ст. 6724.

[6] Федеральный закон от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации» // СЗ РФ. 2010. № 49. Ст. 6422.

систем, входящих в систему обязательного медицинского страхования. Следующий шаг состоит в большей интеграции этих систем и включении в данный механизм других субъектов.

Во-вторых, требуется обеспечение мобильности и динамичности данных, обрабатываемых в информационных системах. Сведения, хранящиеся в информационных системах здравоохранения, должны быть всегда доступны для использования лицами с законным интересом и регулярно актуализироваться.

В-третьих, необходимо расширять область полезного использования информационных систем, в том числе через возможность подключения к этим системам третьих лиц, предлагающих инновационные решения в телемедицине.

В-четвертых, внимание должно уделяться обеспечению прав доступа граждан к персональным электронным записям, хранящимся в информационных системах, включая полномочия по управлению информацией. Такой доступ может быть организован через механизм личного электронного кабинета с удобным и функциональным интерфейсом.

Осознание важности перечисленных факторов уже нашло частичное отражение в законопроектной деятельности органов государственной власти. Министерство здравоохранения РФ представило для общественного обсуждения законопроект[7], направленный на урегулирование отдельных аспектов использования телемедицинских технологий. В целом данный законопроект обладает рядом несомненных преимуществ, поскольку закрепляет долгожданные правовые конструкции, без которых невозможно развитие телемедицины: дается определение телемедицинским технологиям, указывается на возможность оказания медицинских услуг с их применением, устанавливаются организационно-правовые основы единого информационного пространства, необходимого для безопасного взаимодействия субъектов телемедицинских отношений (включая участников системы частного здравоохранения). Кроме того, законопроект расширяет область полезного использования информационных систем здравоохранения, включая возможность динамического наблюдения за изменением состояния здоровья граждан с социально значимыми заболеваниями.

Вместе с тем, большое количество правовых аспектов, связанных с развитием телемедицины, остались за рамками этого законопроекта либо не получили достаточной степени проработки. Данный тезис также подтверждается отрицательным заключением Минэкономразвития РФ по результатам оценки регулирующего воздействия указанного законопроекта[8]. Серьезным пробелом законопроекта, среди прочего, является отсутствие каких-либо положений, направленных на приведение законодательства о защите персональных данных в соответствие с потребностями функционирования телемедицинских технологий.

Важность вопросов адаптации правового режима персональных данных к условиям развития телемедицины признается во многих странах, где активно внедряются достижения электронной медицины[9]. Однако даже в рамках нового европейского регулиро-

---

[7] Проект Федерального закона «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационно-телекоммуникационных технологий в сфере охраны здоровья граждан и создания национальных научно-практических медицинских центров» // http://regulation.gov.ru/projects#npa=46654 (дата обращения: 16.08.2016).

[8] http://regulation.gov.ru/Files/GetFile?fileid=24a90603-0098-4e20-a04e-5446cc8e9256 (дата обращения: 16.08.2016).

[9] См. *Gilroy A., Spontoni C., Llewellyn K., Undine von Diemar.* Data protection challenges for telemedicine in the EU and US // E-Health Law & Policy. 2015. Vol. 2. Issue 8. P. 12–14.

вания в области защиты персональных данных, вступающего в силу на всей территории ЕС с 25 мая 2018 г.[10], обозначенная проблема не получила своего окончательного решения, что при этом не лишает ее актуальности, а только усиливает потребность в поиске оптимальной модели регулирования[11].

Проблемные аспекты применения действующего законодательства о персональных данных к телемедицинским отношениям включают требования конкретного, информированного согласия на обработку персональных данных; закрепление специальных условий обработки персональных данных субъектами телемедицинской деятельности; требования к обеспечению безопасности информационных систем, в которых обрабатываются персональных данные при осуществлении телемедицинской деятельности.

Проблема получения согласия на обработку персональных данных является, пожалуй, наиболее острой и дискуссионной. Краеугольным камнем данной проблемы можно назвать требование конкретности данного согласия. Поскольку в телемедицине обрабатываются преимущественно сведения о здоровье, то задача получения согласия усложняется также необходимостью соблюдения письменной формы с целым рядом дополнительных формальностей[12].

Некоторые авторы[13] справедливо высказывают мнение, что по мере развития технологий дистанционной обработки персональных данных соблюдение требования к информированному конкретному согласию становится исключительно формальным и не обеспечивает подлинной реализации автономии воли человека. В результате необходимость соблюдения всех формальностей превращается из гарантий права на неприкосновенность личности в дополнительные барьеры для распространения и использования новых технологий. В телемедицине это проявляется с особенной остротой.

Российское законодательство закрепляет существенные барьеры для свободной передачи и дальнейшей обработки сведений о состоянии здоровья граждан. В условиях развития телемедицинских технологий соблюдение всех этих требований является затруднительным и не всегда представляется возможным. К наиболее сложным для соблюдения можно отнести следующие требования:

• конкретного согласия в отношении перечня персональных данных, целей обработки, действий с персональными данными;

---

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // OJ L 119, 4.5.2016. P. 1–88 // http://eur-lex.europa.eu/eli/reg/2016/679/oj (дата обращения: 16.08.2016).

[11] См.: *Hordern V.* Will the New EU Data Protection Regulation Facilitate Healthcare Innovation? // Chronicle of Data Protection, 26 January 2015 // http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/will-eu-data-protection-regulation-facilitate-healthcare-innovation/ (дата обращения: 16.08.2016); *Hordern V.* The Final GDPR Text and What It Will Mean for Health Data// Chronicle of Data Protection, 20 January 2016 // http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ (дата обращения: 16.08.2016).

[12] Российское законодательство предъявляет к обработке специальных категорий персональных данных более жесткие требования по сравнению с законодательством ЕС, которое указывает на необходимость получения не обязательно письменного, а явно выраженного (explicit) согласия. Подробнее см. разъяснения Рабочей группы ЕС по персональным данным: Article 29 Data Protection Working Party. Opinion 15/2011 on the definition of consent. P. 25 // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (дата обращения: 16.08.2016).

[13] См., напр.: *Mantovani E., Quinn P.* mHealth and data protection — the letter and the spirit of consent legal requirements // International Review of Law, Computers & Technology. Volume 28. 2014. Issue 2. P. 222.

- письменной формы согласия;
- к указанию реквизитов документов субъекта персональных данных
- к перечислению конкретных обработчиков персональных данных и ряд других обязательных к соблюдению положений ФЗ «О персональных данных»[14].

Реализация потенциала телемедицинских технологий не всегда предполагает возможность заранее определить конкретный перечень персональных данных, цели и способы их обработки[15]. В особенности это касается обработки персональных данных в медицинских исследованиях. Перечень персональных данных, цели и способы их обработки в телемедицине имеют динамический характер, что с формальной точки зрения ставит вопрос о необходимости регулярного предоставления согласия субъекта персональных данных.

Письменное согласие также может быть дано в форме электронного документа, подписанного электронной подписью в соответствии с ФЗ «Об электронной подписи»[16]. Законодательство не уточняет, какой вид электронной подписи может использоваться для представления согласия, из чего можно сделать вывод, что достаточно использовать простую электронную подпись. Это значительно облегчает дистанционное предоставление согласия, хоть и не исключает необходимости генерации кодов и паролей, посредством которых осуществляется идентификация лица, подписывающего электронный документ.

Требование указания полных реквизитов основного документа, удостоверяющего личность субъекта персональных данных, представляется явно излишним. Во-первых, данное требование нагружает субъектов информационного взаимодействия обременениями, имеющими сомнительную необходимость для обеспечения информированного согласия. Во-вторых, законодательство обязывает предоставлять эти весьма «чувствительные» сведения даже в том случае, когда субъект персональных данных не желает их предоставлять оператору, и при этом оператор не нуждается в этих сведениях для достижения целей обработки персональных данных.

Наконец, указание в согласии на обработку персональных данных конкретных лиц (наименование или ФИО, адрес), которым оператор поручает обработку персональных данных, также создает определенные трудности. В частности, технически в обработке персональных данных могут быть задействованы разные средства, находящиеся в ведении разных субъектов, состав которых и юридические сведения о которых также могут изменяться.

Таким образом, возможности по обработке персональных данных с письменного согласия субъекта в условиях развития телемедицины, предполагающей обработку больших объемов динамической информации, существенно ограничены рамками действующего законодательства.

---

[14] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006, № 31 (1 ч.). Ст. 3451 (далее — ФЗ «О персональных данных»).

[15] Данный тезис справедлив в отношении многих современных технологий, объединяемых понятием технологий обработки Больших данных (Big Data), которые также могут использоваться в медицине. Подробнее о проблемных аспектах применения законодательства о персональных данных к технологиям обработки Big Data см.: *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–67.

[16] Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // СЗ РФ. 2011. № 15. Ст. 2036.

Для решения этой проблемы возможны два пути развития законодательства: 1) фундаментальный, связанный с пересмотром принципов и условий обработки персональных данных; 2) ситуативный, предполагающий включение в законодательство исключений для специального урегулирования конкретных правоотношений (а именно — отношений по обработке персональных данных в телемедицине).

Реализация первого подхода требует системного переосмысления законодательства о персональных данных, на что необходимо затратить серьезные интеллектуальные и организационные ресурсы. Представляется, что в долгосрочной перспективе данный подход окажется предпочтительным, поскольку современные информационные технологии, изменяющие парадигму информационного взаимодействия субъектов[17], будут проникать во все большее количество сфер общественных отношений. В конце концов, настанет момент, когда ситуативными способами решить проблему защиты персональных данных будет невозможно и потребуется системное изменение законодательства.

Тем не менее, на данном этапе вопрос о защите персональных данных в телемедицине можно и нужно решать посредством специального регулирования. ФЗ «О персональных данных» уже содержит механизмы, позволяющие предусматривать в законодательстве исключения из применения общих требований. Более того, в законе есть немало исключений, список которых регулярно пополняется, что также свидетельствует о кризисном состоянии действующей модели правовой защиты персональных данных.

Применительно к медицинской сфере в ФЗ «О персональных данных» предусмотрены исключения, разрешающие обработку персональных данных без согласия субъекта в следующих случаях: 1) обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно; 2) обработка специальной категории персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну; 3) обработка специальной категории персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством; 4) обработка персональных данных осуществляется в статистических или иных исследовательских целях при условии обязательного обезличивания персональных данных.

Закономерно возникает вопрос о достаточности перечисленных исключений для обработки персональных данных в телемедицинских целях. Представляется, что указанных исключений в их нынешней формулировке явно недостаточно для легитимации обработки персональных данных в телемедицине без согласия субъекта персональных данных. Кроме того, разнообразие способов использования телемедицинских технологий и необходимость уважения автономии воли человека не вписываются в жесткое дихотомическое деление «с согласием — без согласия».

Конечно, осуществление отдельных видов телемедицинской деятельности вполне могло бы вписаться в уже предусмотренные случаи обработки персональных данных без согласия пациента (например, в случае необходимости оказания экстренной медицинской помощи). Однако существенная часть телемедицины, особенно ее наиболее

[17] Подробнее см.: *Birnhack M.* S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm (August 15, 2013). Big Data and Privacy: Making Ends Meet 7–10 (Future of Privacy Forum & Center for Internet & Society, Stanford Law School) (2013) // http://ssrn.com/abstract=2310700 (дата обращения: 16.08.2016).

инновационная сфера (например, использование «Интернета вещей» для дистанционного наблюдения за пациентами), остается за пределами регулирования. Даже возможности по осуществлению медицинских исследований при обезличивании персональных данных сталкиваются с серьезными ограничениями[18].

В связи с этим можно предусмотреть в ч. 1 ст. 6 и ч. 2 ст. 10 ФЗ «О персональных данных» дополнительное основание для обработки персональных данных — «обработка персональных данных осуществляется субъектами телемедицинской деятельности в целях оказания телемедицинских услуг и осуществления научных и статистических исследований с использованием телемедицинских технологий».

Имплементация подобных положений в ФЗ «О персональных данных» должна осуществляться системно, с одновременным изменением положений ФЗ «Об основах охраны здоровья граждан в Российской Федерации». В частности, следует закрепить понятие телемедицинских услуг, телемедицинских технологий, определить субъектов телемедицинской деятельности, включить основания для предоставления сведений, составляющих врачебную тайну, субъектам телемедицинской деятельности с обязательством соблюдать конфиденциальность полученных сведений.

Примечательно, что в альтернативном законопроекте о телемедицине, разработанном Фондом развития Интернет-инициатив и некоторыми представителями Интернет-индустрии[19], предусмотрены многие из вышеперечисленных положений. Закреплены понятия телемедицины, телемедицинской услуги. Более того, предложены изменения в ст. 10 ФЗ «О персональных данных», разрешающие обработку специальных категорий персональных данных в целях организации оказания телемедицинских услуг при условии, что обработка персональных данных осуществляется лицом, обязанным в соответствии с законом сохранять их конфиденциальность. Тем не менее, проект закона в данном виде пока не продвинулся на следующие этапы законотворческого процесса, хотя и обсуждается на государственном уровне совместно с представителями IT-индустрии[20].

Рассмотренная модель законодательного регулирования отношений, связанных с обработкой персональных данных в телемедицине, не лишена недостатков. Ее концептуальный недостаток состоит в игнорировании воли субъекта персональных данных. Законодатель самостоятельно определяет, что любые персональные данные могут обрабатываться в телемедицинских целях без согласия граждан. По факту мы получим переход из одной крайности в другую. Вновь встанет вопрос о легитимности новой модели правового регулирования.

Представляется, что подходы к согласию субъекта персональных данных на их обработку должны быть дифференцированы не в зависимости от вида персональных дан-

---

[18] При обработке большого массива персональных данных современными технологиями полное обезличивание представляется трудно достижимым ввиду деобезличивающего (индивидуализирующего) потенциала таких технологий. Подобная мысль была изложена еще в 2007 года в отчете Рабочей группы ЕС по персональным данным: Opinion 4/2007 on the Concept of Personal Data, WP136 (2007). P. 18 // http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (дата обращения: 15.05.2016). Подробнее о влиянии технологий Big Data на возможность обезличивания персональных данных см.: *Santos J.* The Myth of Anonymization: Has Big Data Killed Anonymity? // Kantar Health, March 2015 // http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (дата обращения: 16.08.2016).

[19] О разработке законопроекта см.: Телемедицина ждет своего рецепта // http://www.kommersant.ru/doc/2882970 (дата обращения: 16.08.2016).

[20] Законопроект о телемедицине обсудили на заседании в Госдуме // http://www.vesti.ru/doc.html?id=2755645 (дата обращения: 16.08.2016).

ных (обычные или специальные), а в зависимости от наличия публичного интереса в обработке тех или иных персональных данных. При наличии публичного интереса со стороны большого количества субъектов законодатель может избрать две модели регулирования:

1) разрешить обработку персональных данных вне зависимости от согласия субъекта;

2) разрешить обработку персональных данных без согласия субъекта до тех пор, пока субъект не выразит несогласия с обработкой персональных данных (модель «*opt-out*»[21]).

Обе модели могли бы использоваться для реализации публичных интересов и дифференцироваться в зависимости от конкретных целей и потребностей с учетом разумного и достаточного ограничения воли субъектов персональных данных.

Что касается необходимости защиты более чувствительных данных, то здесь ключевую роль должно играть не письменное согласие субъекта, которое не предоставляет более надежных гарантий защиты персональных данных, а повышенные стандарты безопасности, которые обязаны соблюдать операторы/обработчики таких данных. В законодательстве уже предусмотрена дифференциация требований к защите информационных систем в зависимости от потенциальных угроз, которые, в том числе определяются видом персональных данных, обрабатываемых в этих системах[22]. Существующее разграничение формы согласия в зависимости от вида обрабатываемых данных создает лишние препятствия при осуществлении разных видов деятельности и трудности с толкованием законодательства[23], особенно, когда обработке подлежат одновременно обычные и специальные категории персональных данных.

Другим важным вопросом защиты персональных данных в телемедицине, тесно связанным с требованием к согласию на обработку, является закрепление круга субъектов телемедицинской деятельности, участвующих в обработке персональных данных. Распространение различных мобильных устройств в медицине, функционирование медицинских онлайн-сервисов, внедрение облачных технологий в медицину, использование технологий обработки больших данных вовлекает в эту сферу все больше новых субъектов (провайдеров доступа к Интернету, хостинг-провайдеров, администраторов сайтов, операторов облачных сервисов, производителей IT-устройств, фармацевтические компании, платежные системы и т.д.). Многие из этих субъектов тем или иным образом связаны с обработкой персональных данных пациентов.

Закон «О персональных данных» по общему правилу не содержит ограничений в отношении фигуры оператора/обработчика персональных данных. Обрабатывать сведения о пациентах могут любые лица при соблюдении принципов и условий обработки персональных данных. Вместе с тем, в рамках телемедицины встает вопрос о специаль-

---

[21] В п. 2 ст. 9 ФЗ «О персональных данных» предусмотрена возможность отзыва согласия на обработку персональных данных. Однако в законе отдельно оговаривается, что оператор вправе продолжить обработку персональных данных при наличии оснований, разрешающих их обработку без согласия субъекта персональных данных. Таким образом, в российском законодательстве о персональных данных не предусмотрена модель «opt-out» как способ получения согласия на их обработку.

[22] Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» // СЗ РФ. 2012. № 45. Ст. 6257.

[23] Следует отметить проблему соотношения условий обработки обычных и специальных персональных данных. Из буквального толкования закона можно сделать вывод, что условия обработки специальных персональных данных дополняют условия обработки обычных персональных данных. Однако системное и телеологическое толкование приводит к заключению, что имеет место не дополнение, а замена одних условий другими.

ном урегулировании возможности обработки персональных данных субъектами телемедицинской деятельности.

На сегодняшний день в российском законодательстве в качестве специальных субъектов обработки персональных данных в медицине можно выделить лиц, профессионально занимающихся медицинской деятельностью и обязанных сохранять врачебную тайну, и субъектов отношений в области медицинского страхования (следует из п. 8 ч. 2 ст. 10 ФЗ «О персональных данных»). Очевидно, что для легитимации обработки персональных данных в телемедицинских целях требуется законодательное закрепление статуса субъектов телемедицинской деятельности[24]. При этом на отдельные субъекты могут быть наложены дополнительные обязанности (специальные требования по аккредитации, к обеспечению конфиденциальности, уведомлению об утечках информации, хранению персональных данных[25] и т.п.).

Наконец, еще один важный блок вопросов, связанный с защитой персональных данных в телемедицине, касается обеспечения безопасности информационных систем персональных данных, используемых в телемедицине.

Защита любой конфиденциальной информации требует применения целого комплекса правовых, организационных и технических мер защиты. При этом уровни безопасности и соотношение этих мер должны зависеть от многих факторов: объема обрабатываемых данных, степени чувствительности данных, количества лиц, имеющих доступ к данным, добровольности/обязательности передачи данных в обработку, динамизма/статичности данных, хранящихся в базе и т.п. Информационные системы персональных данных, используемых в телемедицине, обладают такими характеристиками, которые требуют наибольшего уровня защиты. Важнейшими задачами обеспечения безопасности информационных систем в телемедицине являются: предоставление доступа к персональным записям о здоровье граждан только лицам с законным и обоснованным интересом (в том числе внутри медицинской организации); обеспечение физической безопасности IT-инфраструктуры, используемой в телемедицине; применение технологий шифрования информации при ее передаче по каналам связи[26] и др.[27]

В Российской Федерации нормативно-правовая база в области защиты информационных систем персональных данных о пациентах включает в себя отдельные положения

---

[24] Например, в США после реформы 2009 года требования к обработке персональной информации о здоровье, установленные актом HIPPA, были распространены на новые субъекты — бизнес-партнеры (business entities), предлагающие инновационные решения в области электронного здравоохранения. Подробнее см.: *Gantt W. (Editor), ABA Health Law Section.* E-Health, Privacy, and Security Law, Second Edition, Cumulative Supplement. BNA Books, 2015. P. 73.

[25] Некоторые авторы высказывают небесспорные предложения о необходимости хранения персональных данных о состоянии здоровья граждан только на локальных внутренних серверах конкретного государства (по сути, речь идет о локализации таких данных, что уже предусмотрено в российском законодательстве в отношении любых персональных данных граждан РФ). См.: *Daly A.* The law and ethics of 'self-quantified' health information: An Australian perspective // International Data Privacy Law. 2015. 5(2). P. 154.

[26] К перспективным технологиям шифрования чувствительной информации относятся гомоморфные алгоритмы шифрования данных, когда информация передается отдельными зашифрованными пакетами через независимые линии связи. Подробнее см.: https://issek.hse.ru/trendletter/news/172112565.html (дата обращения: 16.08.2016).

[27] О других механизмах обеспечения информационной безопасности в электронном здравоохранении см.: *Hongyang Yan, Jin Li, Xuan Li, Gansen Zhao, Sun-Young Lee, and Jian Shen.* Secure Access Control of E-Health System with Attribute-Based Encryption // Intelligent Automation & Soft Computing. 2006. Vol. 22. N 3. P. 345–352.

ФЗ «О персональных данных» (главным образом, ст. 19), ряд подзаконных актов[28], в том числе отраслевого характера[29]. Данные акты закрепляют широкий перечень организационных, правовых и технических требований, которые должны соблюдать операторы персональных данных. Однако, как отмечают эксперты, соблюдение большого массива требований законодательства на практике является формальным, ввиду чего реальный уровень безопасности информационных систем здравоохранения гораздо ниже, чем заявленный в документах[30]. Медицинские информационные системы нуждаются в качественно новом уровне защищенности[31], обеспечивающем надежность функционирования современных телемедицинских технологий.

Частями 5 и 6 ст. 19 ФЗ «О персональных данных» предусмотрена возможность для отраслевых органов государственной власти, а также ассоциаций, союзов и иных объединений операторов определять дополнительные угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении деятельности в определенной сфере. Таким образом, на уровне закона вопросы защиты медицинских информационных систем урегулированы в общем виде — установлен общий правовой режим безопасности персональных данных. Специальный правовой режим безопасности медицинских информационных систем должен устанавливаться отраслевым сообществом с учетом специфических угроз и особенностей функционирования телемедицинских технологий.

В заключение следует подчеркнуть, что развитие телемедицинских технологий обязательно должно сопровождаться комплексным правовым обеспечением. При этом не стоит недооценивать важность правовых аспектов защиты персональных данных в телемедицине. От выработанных подходов к защите персональных данных напрямую зависит доверие общества к телемедицине и готовность бизнеса к предложению инновационных решений в здравоохранении.

Рассмотренные на примере телемедицины проблемы адаптации правового режима персональных данных к современным технологиям ставят фундаментальный вопрос о жизнеспособности действующей модели правовой защиты персональных данным. Сможет ли данная модель пережить переход к качественно новому формату информационного взаимодействия либо ее место займет другая модель — это вопрос открытый. Ответ на него во многом зависит от совместных усилий академического сообщества, переосмысляющего состояние правовых институтов в цифровую эпоху[32].

---

[28] Напр., Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» // Российская газета. № 107. 2013.

[29] «Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости» (утверждены Минздравсоцразвития 23.12.2009) // http://docs.cntd.ru/document/902301906 (дата обращения: 16.08.2016).

[30] http://www.cnews.ru/reviews/it_v_zdravoohranenii/articles/kak_zashchitit_persdannye_v_bolnitse/ (дата обращения: 16.08.2016).

[31] О необходимости разработки новых подходов к обеспечению информационной безопасности в новой технологической парадигме см.: *Bainbridge D.* Introduction to Information Technology Law. 6th Edition. Trans-Atlantic Publications. 2008. P. 635–636.

[32] См. напр., *Терещенко Л.К.* Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2013. 227 с.

Библиография

Богдановская И.Ю. Правовое регулирование телемедицины: опыт США // Врач и информационные технологии. 2007. № 3. С. 64–68.

Наумов В.Б., Савельев Д.А. Правовые аспекты телемедицины. СПб.: Анатолия, 2002. 107 с.

Савельев А.И. Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–67.

Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография. М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, ИНФРА-М, 2013. 227 с.

Штыкова Н.Н. Сущность и проблемы реализации электронной медицины (на примере Владимирской области) // Медицинское право. 2014. № 5. С. 22–27.

Gilroy A., Spontoni C., Llewellyn K., Undine von Diemar. Data protection challenges for telemedicine in the EU and US // E-Health Law & Policy. 2015. Vol. 2. Issue 8. P. 12–14.

Birnhack M. S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm (August 15, 2013). Big Data and Privacy: Making Ends Meet 7–10 (Future of Privacy Forum & Center for Internet & Society, Stanford Law School) (2013) // http://ssrn.com/abstract=2310700 (дата обращения: 16.08.2016).

Daly A. The law and ethics of 'self-quantified' health information: An Australian perspective // International Data Privacy Law. 2015. 5(2). P. 144–155.

Bainbridge D. Introduction to Information Technology Law. 6th Edition. Trans-Atlantic Publications, 2008. 665 p.

Mantovani E., Quinn P. mHealth and data protection — the letter and the spirit of consent legal requirements // International Review of Law, Computers &Technology. Volume 28. 2014. Issue 2. P. 222–236.

Carlisle G., Whitehouse D., Penny D. (Eds.). eHealth: Legal, Ethical and Governance Challenges. Springer, 2013. XII, 396 p.

Hongyang Yan, Jin Li, Xuan Li, Gansen Zhao, Sun-Young Lee and Jian Shen. Secure Access Control of E-Health System with Attribute-Based Encryption // Intelligent Automation & Soft Computing. 2006. Vol. 22. № 3. P. 345–352.

Santos J.. The Myth of Anonymization: Has Big Data Killed Anonymity? // Kantar Health, March 2015 // http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (дата обращения: 16.08.2016).

Hordern V. The Final GDPR Text and What It Will Mean for Health Data // Chronicle of Data Protection, 20 January 2016 // http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ (дата обращения: 16.08.2016).

Gantt W. (Editor), ABA Health Law Section. E-Health, Privacy and Security Law. Second Edition, Cumulative Supplement. BNA Books, 2015. 538 p.

Personal Data Protection in Telemedicine

Mikhail S. Zhuravlev

Junior Research Fellow, International Laboratory for Information Technology and Intellectual Property Law, National Research University Higher School of Economics. Address: 20 Myasnitskaya Str., Moscow 101000, Russian Federation. E-mail: mzhuravlev@hse.ru

Abstract

The relevance of personal data protection in telemedicine is predetermined by the rapid development of information technologies in different spheres, including health care. The key issue is that current legal framework for personal data protection does not adequately meet the needs of telemedicine. Rather than facilitating technological development the law creates unreasonable barriers for introducing innovations in health care. Modern information and communication technologies require a free, secure and legitimate information exchange among all actors of telemedicine relationships. The ar-

ticle contains recommendations on improving legislation on personal data for facilitating telemedicine development. The paper mainly focuses on the principles of personal data protection in telemedicine (requirements for informed consent, purposes of processing, special rules for data controllers and data processors, obligations to ensure confidentiality and security etc.). In particular, it is proposed to eliminate the mandatory requirement of written consent for processing special categories of personal data; to establish special grounds for personal data processing in telemedicine purposes; to differentiate the processing of personal data in telemedicine depending on the consent requirement ("without consent" "without consent, but with option to refuse processing", "with consent"). It is necessary to set the legal status of telemedicine entities and possibly impose special obligations for personal data processing performed by these entities. In addition, it is important to establish industry standards for security of health information systems taking into account specific threats typical to telemedicine technologies. The article also focuses on the Russian legislative approach to health information systems that are crucial for telemedicine. The thesis is supported that legislation in this area should facilitate integration and interoperability of health information systems, expand applicability of these systems and increase the role of patients in management of personal electronic health records. The methodological basis of the research includes analysis of legislation and draft laws on corresponding issues, comparative legal method (in some aspects Russian experience is considered in comparison with experience of the EU and USA) and method of legal modeling (amendments to Russian legislation are proposed).

Keywords

telemedicine; e-health; personal data; information security; health information systems; legislation on personal data; consent to personal data processing; Internet of things; Big Data.

Citation: Zhuravlev M.S. (2016) Personal Data Protection in Telemedicine. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 3, pp. 85–94 (in Russian)

DOI: 10.17323/2072-8166.2016.3.72.84

References

Bainbridge D. (2008) *Introduction to Information Technology Law*. Trans-Atlantic Publications, 665 pp.

Birnhack M. (2013) S-M-L-XL Data: Big Data as a New Informational Privacy Paradigm (August 15, 2013). *Big Data and Privacy: Making Ends Meet 7-10 (Future of Privacy Forum & Center for Internet & Society, Stanford Law School)*. Available at: http://ssrn.com/abstract=2310700 (accessed 16 August 2016).

Bogdanovskaya I.Yu. (2007) Pravovoe regulirovanie telemeditsiny: opyt SShA [Legal Regulation in E-medicine: Case of US]. *Vrach i informatsionnye tekhnologii*, no 3, pp. 64-68.

Carlisle G., Whitehouse D., Duquenoy P. (Eds.) (2013) *eHealth: Legal, Ethical and Governance Challenges*. Springer. XII, 396 pp.

Daly A. (2015) The law and ethics of 'self-quantified' health information: An Australian perspective. *International Data Privacy Law*, 5(2), pp 144-155.

Gantt III W. A. H. (Editor) (2015) *ABA Health Law Section*. E-Health, Privacy, and Security Law, Second Edition, Cumulative Supplement. BNA Books, 538 pp.

Gilroy A., Spontoni C., Llewellyn K., von Diemar U. (2015) Data protection challenges for telemedicine in the EU and US. *E-Health Law & Policy*. Vol. 2. Issue 8. pp. 12-14.

Hongyang Y., Li J., Li. Xuan, Z. Gansen, Lee S., Shen J. (2006) Secure Access Control of E-Health System with Attribute-Based Encryption. *Intelligent Automation & Soft Computing*. Vol. 22, no 3, pp. 345–352.

Hordern V. (2015) Will the New EU Data Protection Regulation Facilitate Healthcare Innovation? *Chronicle of Data Protection*. Available at: http://www.hldataprotection.com/2015/01/articles/international-eu-privacy/will-eu-data-protection-regulation-facilitate-healthcare-innovation/ (accessed 16 August 2016);

Hordern V. (2016) The Final GDPR Text and What It Will Mean for Health Data. *Chronicle of Data Protection*. Available at: http://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/ (accessed 16 August 2016).

Mantovani E., Quinn P. (2014) mHealth and data protection — the letter and the spirit of consent legal requirements. *International Review of Law*, Computers &Technology. Volume 28, issue 2. pp. 222–236.

Naumov V.B., Savel'ev D.A. (2002) *Pravovye aspekty telemeditsiny* [Legal Aspects of Telemedicine]. Saint Petersburg: Anatoliya, 107 p. (in Russian)

Santos J. (2015) The Myth of Anonymization: Has Big Data Killed Anonymity? *Kantar Health*. Available at: http://www.kantarhealth.com/docs/white-papers/the-myth-of-anonymization-has-big-data-killed-anonymity-.pdf (accessed 16 August 2016).

Savel'ev A. I. (2015) Problemy primeneniya zakonodatel'stva o personal'nykh dannykh v epokhu "Bol'shikh dannykh" (Big Data) [The Issues of Implementing Legislation on Personal Data in the Era of Big Data]. *Pravo. Zhurnal Vysshey shkoly ekonomiki*, no 1, pp. 43–67.

Shtykova N.N. (2014) Sushchnost' i problemy realizatsii elektronnoy meditsiny (na primere Vladimirskoy oblasti). *Meditsinskoe pravo*, no 5, pp. 22–27.

Tereshchenko L.K. (2013) *Modernizatsiya informatsionnykh otnosheniy i informatsionnogo zakonodatel'stva: monografiya* [Updating Information Relations and Information Legislation. Monograph]. Moscow: Institut zakonodatel'stva i sravnitel'nogo pravovedeniya pri Pravitel'stve RF, INFRA-M, 227 p. (in Russian)