

Интероперабельность как фактор развития права в сфере электронного здравоохранения



М.С. Журавлев

преподаватель департамента общих и межотраслевых юридических дисциплин факультета права Национального исследовательского университета «Высшая школа экономики». Адрес: 101000, Российская Федерация, Москва, ул. Мясницкая, 20. E-mail: mzhuravlev@hse.ru



Аннотация

Развитие электронного здравоохранения в условиях цифровой экономики требует информационного взаимодействия всех заинтересованных субъектов. Такое взаимодействие обеспечивается посредством интероперабельности информационных систем, данных, технических решений, процессов и методов управления. В интероперабельной информационной среде достигается синергетический эффект от взаимодействия, при котором каждый участник получает пользу от использования данных и повышает эффективность своей деятельности. Интероперабельность необходима для создания единого безбарьерного информационного пространства, основанного на принципах открытости, прозрачности, многоцелевого использования данных, технологической нейтральности, приоритета интересов пользователей, информационной безопасности и защиты неприкосновенности частной жизни. В статье раскрываются принципы интероперабельности, применимые к сфере электронного здравоохранения, со ссылками на опыт Европейского союза, где концепция интероперабельности получила наибольшее развитие. Каждый из принципов рассматривается через призму правовых вопросов, которые необходимо учитывать в процессе их имплементации. Отдельное внимание уделяется вопросам стандартизации, требованиям к информационной безопасности (в том числе безопасности медицинских устройств и приложений), разрешению коллизий между принципом долгосрочного хранения данных в целях повторного их использования и требованиями законодательства о персональных данных. Отмечаются позитивные шаги на пути к нормативно-правовому обеспечению взаимодействия информационных систем здравоохранения в России, где, в частности, созданы условия для развития Единой государственной информационной системы здравоохранения (ЕГИСЗ). Вместе с тем делается акцент на том, что интероперабельность не должна быть изолированной (внутриотраслевой), так как она в широком смысле предполагает открытость взаимодействия с иными информационными системами (межотраслевому взаимодействию), архитектура которых также должна быть выстроена по аналогичным универсальным стандартам. Этой целью обосновывается необходимость разработки единой стратегии развития интероперабельности в Российской Федерации. Такая стратегия требует комплексного подхода на общегосударственном уровне с участием в ее разработке и реализации всех заинтересованных сторон.



Ключевые слова

интероперабельность; оборот данных; электронное здравоохранение; телемедицина; информационные системы; стандартизация; информационная безопасность.

Благодарности: Статья подготовлена в ходе исследования 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».

Для цитирования: Журавлев М.С. Интероперабельность как фактор развития права в сфере электронного здравоохранения // Право. Журнал Высшей школы экономики. 2019. № 3. С. 98–116.

УДК: 34.09

DOI: 10.17-323/2072-8166.2019.3.98.116

Введение

Информация в телемедицине и электронном здравоохранении может собираться из разных источников (в том числе генерироваться без непосредственного участия человека¹ датчиками, сенсорами и прочими устройствами), иметь как структурированный, так и неструктурированный вид, храниться в разных форматах, обрабатываться разными субъектами в различных целях. Отсутствие унифицированных технических, организационных и правовых основ обработки медицинских данных в информационных системах здравоохранения выступает существенным барьером для информационного обмена и успешного развития телемедицины.

В целях устранения этого барьера и достижения синергетического эффекта от информационного взаимодействия необходимо использовать единые стандарты сбора, хранения, обработки и обмена данными, что обеспечит интероперабельность информационных систем [Oemig F., Snelick R., 2016: V]. Интероперабельность призвана создать единую информационную экосистему, в которой все ее участники в целом и каждый из участников в отдельности получали бы дополнительные возможности и преимущества от

¹ В зарубежной правовой литературе и правовых актах названия таких данных — «индустриальные данные», «данные Интернета вещей», «данные, генерируемые машиной» (machine-generated data). Их обработка в цифровой экономике также связана с целым спектром правовых вопросов, касающихся определения имущественных прав на такие данные, а также механизмов доступа к ним заинтересованных третьих лиц [Drexl J., 2016: 1–70]. См. также: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions «Building a European Data Economy». 2017. Available at: URL: <https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy> (дата обращения: 04.05.2019)

использования информации, извлекали пользу и повышали эффективность своей деятельности. Интероперабельность является необходимым условием развития Интернета вещей [Burluson W., Carrara S., 2014: 1–11], «умного города» и других направлений цифровой экономики, основанных на обмене данными [Ahlgren B., Hidell M., Ngai E., 2016: 52–56].

Сформировавшись как принцип взаимодействия информационных систем в технической области, сегодня интероперабельность является не только техническим принципом, но и принципом социального информационного взаимодействия в сфере государственного управления, бизнесе и других сферах общественных отношений, включая здравоохранение. Реализация принципа интероперабельности в различных сферах общественных отношений требует выработки правовых подходов, направленных на защиту прав и законных интересов субъектов взаимодействия. К наиболее важным правовым вопросам, связанным с имплементацией принципа интероперабельности, относятся вопросы стандартизации, обеспечения открытости, технологической нейтральности и информационной безопасности (включая вопросы защиты неприкосновенности частной жизни)

1. Значение интероперабельности в развитии электронного государства

В контексте построения цифровой экономики интероперабельность следует понимать как условие перехода электронного государства на новый этап развития, в котором публичные услуги² не только переводятся в электронный формат, но и получают качественно новое содержание за счет оперативного информационного обмена, дистанционного взаимодействия и внедрения современных технологий обработки данных. В некоторых международных правовых документах предлагается вместо термина «электронное государство» (e-government) в новых условиях использовать термин «цифровое государство» (digital government)³. Акцент в цифровом государстве делается на формировании системы эффективного взаимодей-

² Под публичными услугами понимаются не только государственные услуги. Как отмечает Л.К. Терещенко, «термин «публичные услуги» гораздо шире «государственных услуг», их могут оказывать и государственные, и негосударственные структуры, но главное, что их объединяет, — это заинтересованность общества в их выполнении, общественный интерес, социальная значимость» [Терещенко Л. К., 2004: 16].

³ В Рекомендации Совета ОЭСР по стратегиям цифрового государства (2014) под цифровым государством понимается модель государственного управления, основанная на использовании цифровых технологий (включая аналитику данных) в качестве системного элемента модернизации государственного управления в общественно полезных целях. См. Recommendation of the Council on Digital Government Strategies. 2014. Available at: URL: <http://www.oecd.org/gov/digital-government/Recommendation-digital-government-strategies.pdf> (дата обращения: 27.07.2019)

ствия участников в сфере публичного управления. Интероперабельность выступает ключевым элементом этого взаимодействия. Становление цифрового государства, основанного на интероперабельности, нуждается в комплексном правовом обеспечении, однако действующее отечественное законодательство «по-прежнему существует в терминах электронного правительства» [Талапина Э.В., 2018: 20–25]. Этим объясняется необходимость разработки новых методологических подходов к правовому регулированию.

В России понятие «интероперабельность» раскрывается в национальном стандарте ГОСТ Р 55062-2012⁴, в котором под интероперабельностью понимается способность двух или более информационных систем или компонентов к обмену информацией и к использованию информации, полученной в результате обмена. Данное определение охватывает главным образом технические аспекты взаимодействия, что характеризует его как узкий (технический) подход к интероперабельности. В широком же (социальном) значении интероперабельность представляет собой не стандарт технического взаимодействия информационных систем, а концепцию управления в условиях информатизации общества, реализуемую в рамках государственной политики с участием всех заинтересованных сторон.

Наибольшую разработанность идея интероперабельности в широком значении получила в Европейском союзе в рамках реализации стратегии построения единого цифрового рынка (Digital Single Market)⁵. Под интероперабельностью в правовых документах ЕС⁶ понимается способность органов публичной власти взаимодействовать для достижения взаимовыгодных целей, осуществляя обмен информацией и знаниями. Информационный обмен и взаимодействие осуществляются органами публичной власти как между собой, так и с гражданами и организациями (главным образом в процессе оказания государственных услуг).

В зарубежной литературе, посвященной вопросам интероперабельности⁷, а также в правовых источниках⁸ выделяют четыре уровня интеропера-

⁴ Национальный стандарт Российской Федерации ГОСТ Р 55062-2012 Информационные технологии (ИТ). Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. 2012. URL: <http://docs.cntd.ru/document/1200102958> (дата обращения: 27.07.2019)

⁵ Digital Single Market. 2019. Available at: URL: <https://ec.europa.eu/digital-single-market/> (дата обращения: 07.08.2019)

⁶ European Interoperability Framework. 2017. Available at: URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (дата обращения: 07.08.2019)

⁷ Inter-organisational e-government: From four levels of interoperability to seven dimensions of co-governance. 2015. Available at: URL: <http://liu.diva-portal.org/smash/get/diva2:783907/FULLTEXT01.pdf> (дата обращения: 27.07.2019)

⁸ Malta National ICT Interoperability Framework. 2019. Available at: URL: https://mita.gov.mt/en/Technology/Initiatives/Interoperability/Documents/NIF_framework.pdf (дата обращения: 27.07.2019)

бельности: правовой, организационный, семантический и технический. Все четыре уровня объединяет система управления интероперабельностью (interoperability governance), основы которой закладываются государственной стратегией обеспечения интероперабельности.

Организационный уровень интероперабельности означает упорядочение деятельности участников информационного обмена по общим, согласованным модельным правилам. Данному упорядочению, например, могут способствовать меморандумы о взаимопонимании и соглашения об уровне обслуживания между участниками информационного взаимодействия.

На семантическом уровне интероперабельность обеспечивает точность и удобство восприятия обмениваемой информации участниками информационного взаимодействия. Данная задача может решаться посредством разработки каталогов, словарей, схем, кодификаторов, классификаторов, единых реестров и т.п. В телемедицине семантическая интероперабельность имеет особенно большое значение⁹, поскольку от надежности интерпретации данных (в том числе в автоматизированном режиме) непосредственным образом зависят медицинские решения и физическая безопасность пациентов. Параметры здоровья человека образуют сложную систему, для интерпретации которой в отдельности и в совокупности медицинским специалистам требуются не только знания, но также опыт и индивидуальный подход к пациенту. Вызовом семантической интероперабельности в телемедицине является обучение информационных технологий системной интерпретации данных с учетом индивидуальных характеристик пациентов¹⁰.

Технический уровень интероперабельности включает спецификации к интерфейсу, сервисы интеграции данных, протоколы безопасного обмена данными и т.п. Исторически информационные системы отдельных ведомств формировались «снизу вверх» для решения ведомственных задач, в результате чего образовались фрагментарные «островки» ИТ-систем, которые сегодня нуждаются в технической интеграции. В телемедицине техническая интероперабельность имеет ключевое значения в контексте обеспечения повсеместного доступа к информации о состоянии здоровья [Craft R., 2005: 384–404].

Правовой уровень интероперабельности предполагает возможность субъектов, работающих по различным правовым основаниям, взаимодей-

⁹ Workshop on semantic interoperability prerequisites for efficient e-health systems. 2015. Available at: URL: <http://www.who.int/classifications/terminology/prerequisites.pdf> (дата обращения: 07.05.2019)

¹⁰ Discussion Paper on Semantic and Technical Interoperability. 2012. Available at: URL: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20121107_wd02_en.pdf (дата обращения: 07.05.2019)

ствовать друг с другом. Первым шагом на пути к правовой интероперабельности является ревизия нормативной базы на предмет выявления барьеров к интероперабельности (*interoperability barriers*) — ограничений на использование данных, неоправданных требований к использованию специфических технологий, противоречивые требования к одним и тем же процессам, устаревшие требования к безопасности и т.п. Также на этапе разработки новых нормативно-правовых актов необходимо обеспечивать их согласованность с существующей нормативной базой.

Нормативно-правовое обеспечение интероперабельности в ЕС преимущественно касается взаимодействия публичных информационных систем. Однако в условиях построения цифровой экономики интероперабельность необходима не только в публичном секторе, но и между частными информационными системами.

Интероперабельность в частном секторе может иметь значение не только в качестве взаимовыгодной формы взаимодействия между бизнес-партнерами (например, частными медицинскими организациями), но и в качестве условия для реализации прав и законных интересов иных лиц. Так, интероперабельность частных информационных систем приобретает актуальность в связи с признанием права на переносимость персональных данных (*data portability*) и его закреплением в Общем Регламенте ЕС по защите данных 2016 года (GDPR)¹¹. Переносимость данных подразумевает возможность переносить и повторно использовать информацию из одних приложений и информационных систем в другие, тем самым способствуя обмену данными (*data sharing*), и не допускать «запираания» (*lock-in*) информации в автономных, изолированных системах. Представляется, что с дальнейшим распространением цифровых платформ право на переносимость данных будет утверждаться и развиваться в законодательстве многих стран, поскольку оно тесно связано с защитой прав потребителей, свободой экономической деятельности, защитой конкуренции и иными правовыми институтами. Интероперабельность информационных систем, в свою очередь, является инфраструктурной основой для реализации права на переносимость данных.

С учетом специфики и разнообразия частных информационных систем обеспечение интероперабельности между частными субъектами следует

¹¹ Статья 20 GDPR устанавливает, что субъект персональных данных имеет право получать свои персональные данные, которые он направил оператору, в структурированном, широко используемом и машиночитаемом формате, а также имеет право беспрепятственно переносить эти данные от одного оператора к другому. При этом при наличии технической возможности перенесение персональных данных должно осуществляться напрямую от одного оператора к другому. См.: 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). 2016. Available at: URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата обращения: 27.07.2019)

стимулировать преимущественно средствами «мягкого права» (в форме добровольные стандарты, саморегулирования и т.п.), а не общеобязательными нормативными требованиями. В этом заключается отличие от правового обеспечения интероперабельности в частных отношениях от обеспечения интероперабельности в административных отношениях, нуждающихся в подробной нормативно-правовой регламентации.

Таким образом, интероперабельность в цифровой экономике приобретает не только техническое, но и более широкое социальное содержание. Ключевой областью развития интероперабельности является сфера взаимодействия органов публичной власти между собой, с гражданами и организациями. За счет оперативного информационного обмена, дистанционного взаимодействия и внедрения современных технологий обработки данных электронное государство выходит на новый уровень своего становления. Дальнейшее развитие электронного государства (переход к цифровому государству) и в целом к цифровой экономике с учетом прав и законных интересов участников общественных отношений требует выработки доктринальных подходов к правовому обеспечению интероперабельности, формирования методологии соединения технологий и права в новых технологических и социальных условиях.

2. Правовое обеспечение интероперабельности в сфере электронного здравоохранения

Интероперабельность находится в тесной взаимосвязи с правом. В одних случаях эта взаимосвязь предполагает содействие интероперабельности правовыми средствами, в других — столкновение принципов интероперабельности с охраняемыми правом интересами. Правовые средства, способствующие развитию интероперабельности, включают в себя стандартизацию и техническое регулирование, законодательные требования к открытости, технологической нейтральности и информационной безопасности.

Столкновение принципов интероперабельности с охраняемыми правом интересами имеет место в сфере защиты персональных данных, обрабатываемых в интероперабельных информационных системах. Если в первом случае требуется выработка нормативного регулирования, стимулирующего интероперабельность, то во втором — необходимо обеспечение оптимального баланса интересов с учетом потребностей развития цифровой экономики и права на неприкосновенность частной жизни. С одной стороны, потребности цифровой экономики диктуют необходимость «высвобождения» информации, вовлечения ее в экономические процессы, усиления оборота данных. С другой стороны, в условиях цифровой экономики возрастают ри-

ски информационной безопасности и нарушения частной жизни граждан [Demetrius K., 2014: 259–290]. Обеспечение экономических интересов не должно осуществляться в ущерб интересам безопасности и правам граждан на неприкосновенность частной жизни.

2.1. Стандартизация

Стандарты играют ключевую роль в обеспечении интероперабельности. В документах ЕС¹² выделяются шесть этапов их внедрения: определение необходимых стандартов с учетом имеющихся потребностей; оценка выбранных стандартов на предмет их прозрачности, недискриминационности и т.п.; имплементация стандартов; мониторинг соблюдения стандартов; управление развитием стандартов; документирование стандартов и размещение их в открытых каталогах. Данные этапы являются универсальными и применимы к внедрению стандартов и спецификаций в разных отраслях, включая телемедицину. Такая сложная структура стандартизации призвана обеспечить прозрачность стандартов и предоставить возможность участия в их разработке любым заинтересованным лицам, обладающим необходимыми знаниями и компетенцией.

В сфере электронного здравоохранения различные международные сообщества разрабатывают стандарты взаимодействия информационных систем здравоохранения: «Интеграция организации здравоохранения» (Integrating the Healthcare Enterprise, IHE), «Панель стандартов информационных технологий в сфере здравоохранения» (Healthcare Information Technology Standards Panel, HITSP), «Седьмой уровень здравоохранения» (Health Level Seven, HL7) и др. [Oemig F., Snelick R., 2016: 73–156]. Применение широко распространенных стандартов интероперабельности позволит обеспечить совместимость информационных систем здравоохранения с используемым в телемедицине медицинским оборудованием и устройствами, производимых как в России, так и в других странах. Это позволит в большей степени обеспечить гражданам равный доступ к услугам электронного здравоохранения.

В Евросоюзе реализуются проекты по обеспечению соответствия продуктов и технических решений в сфере электронного здравоохранения международным, региональным и национальным стандартам¹³. В России также

¹² European Interoperability Framework. 2017. Available at: URL: https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf (дата обращения: 07.08.2019)

¹³ См.: Paving the Way for e-Health Interoperability: The EURO-CAS Project Launches Today. 2017. Available at: URL: http://www.ehealthnews.eu/index.php?option=com_content&view=article&id=5130:paving-the-way-for-ehealth-interoperability-the-euro-cas-project-launches-today&catid=72:development&Itemid=229 (дата обращения: 28.07.2019)

приняты некоторые стандарты в сфере электронного здравоохранения (например, установлены правила ведения электронных записей о здоровье¹⁴ и приняты национальные стандарты «Электронная история болезни»¹⁵, «Информатизация здоровья»¹⁶), однако требуется проделать еще долгий путь к обеспечению надлежащего уровня интероперабельности. В первую очередь стандартизация необходима в отношении используемых в телемедицине устройств и приложений [Purtova N., Kosta E., Koops B., 2015: 47–74].

В исследованиях, посвященных анализу телемедицинских приложений для мониторинга хронических заболеваний, отмечается «недостаток коммуникации между гетерогенными системами и их интеграции с электронными записями о здоровье пациентов», в связи с чем необходимо создать общую платформу взаимодействия разных приложений и обеспечить совместимость различных устройств для мониторинга за состоянием здоровья [Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B., 2015: 133–150]. Предлагаются модели интероперабельной инфраструктуры [Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B., 2018: 151–159] и оптимальные технические стандарты [Marcheschi P., 2017: 437–443] для достижения данных целей.

Толчком к развитию стандартов интероперабельности телемедицинских устройств и приложений может стать утверждение специальных государственных программ, содействующих разработке стандартов в сфере электронного здравоохранения с учетом успешного международного опыта.

2.2. Открытость

Тесно связанным со стандартизацией является требование открытости, которое применительно к интероперабельности проявляется в нескольких аспектах.

Во-первых, данное требование касается открытости стандартов в сфере информационного обмена¹⁷. Открытость предполагает участие всех заинтере-

¹⁴ Приказ Минздрава России от 09.01.2018 N 2н «О внесении изменений в приказ Министерства здравоохранения Российской Федерации от 15 декабря 2014 г. N 834н «Об утверждении унифицированных форм медицинской документации, используемых в медицинских организациях, оказывающих медицинскую помощь в амбулаторных условиях, и порядков по их заполнению» (Зарегистрировано в Минюсте России 04.04.2018 N 50614) // СПС Консультант Плюс.

¹⁵ ГОСТ Р 52636-2006. Национальный стандарт Российской Федерации. Электронная история болезни. Общие положения (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 407-ст) // СПС Консультант Плюс.

¹⁶ ГОСТ Р ИСО 21091-2017. Национальный стандарт Российской Федерации. Информатизация здоровья. Службы каталога поставщиков и субъектов медицинской помощи и других сущностей (утв. и введен в действие Приказом Росстандарта от 21.06.2017 N 570-ст) // СПС Консультант Плюс.

¹⁷ Например, в Великобритании с 2013 года разрабатывается система открытых стандартов для правительства (open standards for government). См.: Open standards for government. 2019. Avail-

ресованных лиц в разработке, совершенствовании и общественном обсуждении стандартов/спецификаций, их доступность для любого лица, а также предоставление права на использование этих стандартов/спецификаций на честных, разумных и недискриминационных условиях (FRAND — fair, reasonable and non-discriminatory). В Основах обеспечения интероперабельности в ЕС (2017)¹⁸ проводится аналогия с успешным опытом развития экосистемы сети Интернет на основе открытых стандартов/спецификаций, однако делается оговорка о возможном использовании закрытых (проприетарных) стандартов/спецификаций в тех случаях, где это разумно оправдано (например, в сфере электронного здравоохранения использование закрытых стандартов может диктоваться необходимостью обеспечения высоких стандартов информационной безопасности).

Во-вторых, открытость предполагает, что техническая инфраструктура информационного взаимодействия должна по возможности быть основана на открытом программном обеспечении (open source software), а государство, в свою очередь, должно оказывать поддержку сообществ разработчиков такого программного обеспечения. В российской правовой литературе также поддерживается позиция, что «использование свободного программного обеспечения имеет большое количество преимуществ и может обеспечить независимость формирования и обслуживания государственных баз данных». [Камышанская С.В., 2016: 87]. Однако в этом вопросе также стоит принимать во внимание проблемы информационной безопасности. Использование свободного программного обеспечения в электронном здравоохранении не должно ставить под угрозу стабильность информационных систем здравоохранения.

Еще один аспект открытости в контексте интероперабельности касается раскрытия открытых данных. Под открытыми данными в российском законодательстве понимается информация, размещаемая ее обладателями в Интернете в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования¹⁹. На подзаконном уровне также разработаны типовые условия использования открытых данных²⁰. В ЕС требования к раскрытию открытых данных

able at: URL: <https://www.gov.uk/government/publications/open-standards-for-government> (дата обращения: 07.08.2019)

¹⁸ European Interoperability Framework. 2017. Available at: URL: https://ec.europa.eu/isa2/sites/isa2/files/eif_brochure_final.pdf (дата обращения: 07.08.2019)

¹⁹ Ч. 4 ст. 7 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.). Ст. 3448.

²⁰ Типовые условия использования общедоступной информации, размещаемой в информационно-телекоммуникационной сети «Интернет» в форме открытых данных (утв. протоколом заочного голосования Правительственной комиссии по координации деятельности открытого правительства от 19.09.2016 № 6) // СПС Консультант Плюс.

установлены в Директиве об открытых данных (2019)²¹, недавно сменившей Директиву об информации публичного сектора (2003)²². Правовой режим открытых данных имеет большое значение в контексте развития цифровой экономики, поскольку он позволяет ввести в экономический оборот большие объемы данных из публичного сектора. Однако, несмотря на важную роль открытых данных в контексте построения цифрового государства, идея распространения открытых данных в сфере телемедицины ввиду конфиденциального характера медицинской информации имеет ограниченное применение и касается, главным образом, общих статистических сведений в области здравоохранения. Существенная часть обрабатываемых в телемедицине данных носит чувствительный (конфиденциальный) характер, поэтому сообщение таких данных третьим лицам должно осуществляться в рамках иных правовых механизмов (в соответствии с законодательством о персональных данных и врачебной тайне).

2.3. Многоцелевое использование данных

Идея многоцелевого использования данных (reusability) ввиду специфики телемедицинской деятельности имеет ограниченное применение за пределами здравоохранения. Обмен данными возможен преимущественно внутри отрасли между разными ее участниками (например, между государственными и частными медицинскими организациями). Тем не менее, сама возможность многоцелевого использования ИТ-решений и данных как внутри, так и вне медицинской отрасли, должна быть заложена при построении интероперабельной архитектуры информационных систем, для чего необходимы соответствующие организационные, правовые и технические условия.

Правовые условия многоцелевого использования данных во многом связаны с устранением коллизий с законодательством о персональных данных. Одним из необходимых условий многоцелевого использования данных является долгосрочное хранение информации в целостном виде. Однако выполнение этого условия вступает в противоречие с требованием законодательства о персональных данных, предписывающим уничтожать данные по достижении целей их обработки (storage limitation principle). В телемедицине этот вопрос приобретает особую актуальность, поскольку в информационных системах здравоохранения в основном обрабатываются персональные данные пациентов. Названная коллизия нуждается в законодательном урегу-

²¹ Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. 2019. Available at: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024> (дата обращения: 27.07.2019)

²² Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information. 2003. Available at: URL: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32003L0098> (дата обращения: 27.07.2019)

лировании таким образом, чтобы, с одной стороны, обеспечить долгосрочное хранение и доступ к информации, составляющей персональные данные, с другой — не допустить нарушение прав и законных интересов субъектов персональных данных.

В п. «е» пар. 1 ст. 5 Общего Регламента ЕС о защите данных (2016)²³ содержится исключение из принципа ограничения хранения данных, которое позволяет продолжать хранить данные исключительно в целях архивирования в публичном интересе, в исследовательских и статистических целях с принятием необходимых мер по защите прав и законных интересов субъектов персональных данных. В российском Федеральном законе от 27.07.2006 №152-ФЗ «О персональных данных»²⁴ подобное исключение непосредственно не закреплено, однако оно может быть выведено путем системного толкования законодательства. Есть основания полагать, что названное исключение не является универсальным основанием хранения любых персональных данных в целях многократного использования в контексте интероперабельности. Для хранения данных в указанных целях должно быть либо прямое указание федерального закона, либо непосредственное согласие субъекта персональных данных на такое долгосрочное хранение.

2.4. Интеграция информационных систем

Интеграция и расширение каналов взаимодействия информационных систем в сфере здравоохранения предполагает подключение к единой системе максимального количества поставщиков и пользователей медицинской информации. Модель взаимодействия информационных систем здравоохранения должна предусматривать возможность подключения к данной системе иных субъектов, занимающихся исследовательской деятельностью, предлагающих инновационные решения в сфере здравоохранения и т.п.

В России предприняты некоторые шаги к нормативно-правовому обеспечению интероперабельности в сфере электронного здравоохранения: в федеральном законодательстве установлены основы Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)²⁵; Прави-

²³ 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). 2016. Available at: URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1564943268451&uri=CELEX:32016R0679> (дата обращения: 14.08.2019)

²⁴ СЗ РФ. 2006. № 31 (ч. 1). Ст. 3451.

²⁵ Федеральный закон от 29.07.2017 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» // СЗ РФ. 2017. № 31 (часть I). Ст. 4791.

тельством России разработаны Положение о ЕГИСЗ²⁶ и Правила взаимодействия информационных систем здравоохранения²⁷.

Участниками информационного взаимодействия в рамках ЕГИСЗ являются оператор единой системы (Министерство здравоохранения РФ), поставщики информации в единую систему и пользователи информации, содержащейся в единой системе. ЕГИСЗ включает большое количество подсистем, в том числе различные реестры и регистры медицинских организаций, их работников, электронных документов; подсистемы мониторинга в сфере здравоохранения; подсистемы обезличивания персональных данных; защищенную сеть передачи данных; интеграционные подсистемы. Важную роль в обеспечении интероперабельности информационных систем здравоохранения выполняют интеграционные подсистемы. Данные подсистемы реализуют функции формирования единого хранилища данных, управления базами данных, обеспечения защиты информации (в том числе разграничения прав доступа пользователей единой системы), информационно-технологического взаимодействия подсистем между собой и с иными информационными системами, а также другие функции интероперабельности.

2.5. Технологическая нейтральность

Еще одним важным условием обеспечения интероперабельности является технологическая нейтральность (*technological neutrality*). Она предполагает минимизацию использования специфических технологий и установления специфических технических требований при оказании публичных услуг. Формат оказания услуг должен быть, по возможности, технологически независимым и способным адаптироваться к изменяющемуся технологическому контексту. Принцип технологической нейтральности как недопустимость установления каких-либо преимуществ применения одних информационных технологий перед другими закреплен в п. 8 ст. 3 Федерального закона «Об информации, информационных технологиях и о защите информации»²⁸. Технологическая нейтральность в российской правовой доктрине рассматривается также как принцип электронного документоо-

²⁶ Постановление Правительства России от 05.05.2018 N 555 «О единой государственной информационной системе в сфере здравоохранения» // Официальный интернет-портал правовой информации. 2018. URL: <http://www.pravo.gov.ru> (дата обращения: 27.07.2019)

²⁷ Постановление Правительства России от 12.04.2018 № 447 «Об утверждении Правил взаимодействия иных информационных систем, предназначенных для сбора, хранения, обработки и предоставления информации, касающейся деятельности медицинских организаций и предоставляемых ими услуг, с информационными системами в сфере здравоохранения и медицинскими организациями» // СЗ РФ. 2018. № 17. Ст. 2491.

²⁸ СЗ РФ. 2006. № 31 (ч. 1). Ст. 3448.

борота [Бородин М.В., 2016: 102–109]. Значение данного принципа состоит в недопустимости дискриминации технологий, в ограждении «участников оборота от возможной неопределенности правового регулирования, обусловленной устареванием правовых норм, «заточенных» под определенную технологию, и их неадекватностью применительно к новым жизненным реалиям» [Савельев А.И., 2015: 42–51]. В контексте электронного здравоохранения технологическая нейтральность имеет большое значение, поскольку в данной сфере используются устройства с различными техническими характеристиками, доступ к телемедицинским услугам возможен как с мобильных устройств, так и со стационарного компьютера, в перспективе возможно появление иных форм телемедицинской деятельности (например, связанные с внедрением технологии дополненной реальности).

2.6. Иные принципы

Помимо стандартизации, открытости, технологической нейтральности, информационной безопасности комплексное обеспечение интероперабельности в электронном здравоохранении требует соблюдения иных требований: приоритета интересов пользователей, устранения административных барьеров и недопустимости дублирования сбора идентичной информации; требования инклюзивности и доступности; и др.

Приоритет интересов пользователей (*user-centricity*) предполагает учет потребностей и интересов граждан, выступающих потребителями телемедицинских услуг, в вопросах создания, развития сервисов и способов их предоставления. Среди прочего должна обеспечиваться многоканальность услуг (*multi-channel*) и возможность выбора пользователем среди альтернативных способов получения услуг (*no-wrong-door policy*). Развитие данной идеи в телемедицине предполагает недискриминационный характер личного обращения к врачу и дистанционного сеанса с использованием телемедицинских технологий, если для этого нет объективных препятствий.

Повышение роли пациента в управлении своими электронными записями о здоровье связано с развитием персонализированной медицины [Bodiroga-Vukobrat N., Rukavina D., Pavelić K., Sander G., 2016: 6]. Возможности персонализированной телемедицины способствуют не только реализации права граждан на охрану здоровья, но и исполнению обязанности граждан заботиться о состоянии своего здоровья, закрепленной в ст. 27 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации».

Оказание услуг должно по возможности осуществляться с минимальными административными барьерами, посредством режима «одного окна» (*single point of contact*). В той мере насколько это возможно и не ограниче-

но законодательными требованиями (в том числе нормами о защите персональных данных, о врачебной тайне), пользователь должен сообщать аналогичную информацию только однажды, а уже по системе информационного взаимодействия эта информация при необходимости должна передаваться иным структурам (организациям). При этом у пользователя допустимо запрашивать только ту информацию, которая необходима для получения услуги и не может быть получена из других источников.

В телемедицине большое значение имеет требование инклюзивности и доступности, которое подразумевает учет особенностей лиц с ограниченными возможностями и иными затруднениями при использовании электронных сервисами²⁹. Реализация данного принципа способствует обеспечению равенства в доступе к медицинской помощи.

Заключение

В Российской Федерации к настоящему моменту сделаны существенные шаги на пути к правовому обеспечению интероперабельности информационных систем здравоохранения и интеграции телемедицины в цифровую экономику страны. Однако интероперабельность предполагает не только изолированное взаимодействие информационных систем внутри одной отрасли, но и открытость взаимодействия с иными информационными системами (межотраслевому взаимодействию), архитектура которых также должна быть выстроена по аналогичным стандартам. Обеспечение интероперабельности должно строиться на общей стратегии, выступающей ориентиром для отраслевых стандартов (как это реализуется в ЕС). Общая стратегия развития интероперабельности должна быть направлена не только на обеспечение межведомственного электронного документооборота, а, главным образом, на утверждение новой модели государственного управления, основанной на общности целей и единстве форматов взаимодействия различных субъектов (как публичных, так и частных лиц). Такая стратегия требует комплексного подхода на общегосударственном уровне с участием в ее разработке и реализации всех заинтересованных сторон.

Дальнейшие шаги по нормативно-правовому обеспечению интероперабельности предполагают разработку и утверждение стандартов/специфи-

²⁹ Реализация данного принципа возможна, например, посредством предоставления законным представителям технической возможности действий от имени недееспособных лиц при информационном взаимодействии с субъектами телемедицинской деятельности. Такая возможность, помимо технического обеспечения, требует надлежащего юридического закрепления. Российское законодательство предусматривает возможность передачи информированного согласия на медицинское вмешательство в электронном виде законным представителем пациента (ч.7 ст. 20 ФЗ «Об основах охраны здоровья граждан в Российской Федерации»).

каций в сфере информационного обмена, развитие принципов открытости, прозрачности, доступности и ряда других принципов интероперабельности, которым уделяется большое внимание в практике зарубежных стран. Эффективное взаимодействие информационных систем невозможно без комплексного решения целого ряда правовых вопросов, связанных с правовым режимом обработки персональных данных в публичных целях; правовым обеспечением многоцелевого использования персональных данных; уточнением правового режима открытых данных; определением правового режима данных, генерируемых без участия человека; закреплением правовых оснований обработки обезличенных персональных данных и др.



Библиография

- Бородин М.В. О терминах и принципах в сфере электронного документооборота // Актуальные проблемы российского права. 2016. № 2. С. 102–109.
- Камышанская С.В. Свободное программное обеспечение и информационная безопасность Российской Федерации // Власть закона. 2016. № 3. С. 87–95.
- Талапина Э.В. Правовое регулирование цифрового правительства в России: возможности учета требований ОЭСП // Государственная власть и местное самоуправление. 2018. № 3. С. 20–25.
- Терещенко Л.К. Услуги: государственные, публичные, социальные // Журнал российского права. 2004. № 10. С. 15–23.
- Ahlgren B., Hidell M., Ngai E. Internet of Things for Smart Cities: Interoperability and Open Data IEEE. Internet Computing, 2016, issue 6, pp. 52–56.
- Bodiroga-Vukobrat N., Rukavina D., Pavelić K., Sander G. Personalized Medicine. A New Medical and Social Challenge. New York: Springer, 2016. 278 p.
- Burleson W., Carrara S. (eds.) Security and Privacy for Implantable Medical Devices. Berlin: Springer, 2014. 205 p.
- Craft R. Toward Technical Interoperability in Telemedicine. Telemedicine and e-Health, 2005, no 3, pp. 384–404.
- Demetrius K. Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century. Information Technology and Law Series. Berlin: Springer, 2014. 338 p.
- Drexl J. Designing Competitive Markets for Industrial Data: Between Propertisation and Access. Max Planck Institute for Innovation & Competition Research Paper, 2016, no 16–13, 70 p.
- Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B. Review of current telemedicine applications for chronic diseases. Toward a more integrated system? Innovation and Research in Bio Medical engineering, 2015, issue 3, pp. 133–157.
- Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B. Interoperable Infrastructure and Implementation of a Health Data Model for Remote Monitoring of Chronic Diseases with Comorbidities. Innovation and Research in Bio Medical engineering, 2018, issue 3, pp. 151–159.

Marcheschi P. Relevance of e-Health standards for big data interoperability in radiology and beyond. *La radiologia medica*, 2017, issue 6, pp. 437–443.

Oemig F., Snelick R. *Healthcare Interoperability Standards Compliance Handbook*. Berlin: Springer International Publishing, 2016. 662 p.

Purtova N., Kosta E., Koops B. *Laws and Regulations for Digital Health*. Fricker S., Thümler C., Gavras A. (eds.) *Requirements Engineering for Digital Health*. Springer, 2015, pp. 47–74.

Pravo. Zhurnal Vyshey Shkoly Ekonomiki. 2019. No 3

Interoperability as Factor of Law Development in the Digital Economy (eHealth Case)



Michail Zhuravlev

Lecturer, Department of General and Special Branches of Sciences, Law Faculty, National Research University Higher School of Economics. Address: 20 Myasnitsky Str., Moscow 101000, Russia. E-mail: mzhuravlev@hse.ru



Abstract

The development of eHealth in the digital economy requires a comprehensive information exchange between all stakeholders. This interaction is ensured through the interoperability of information systems, data, technical solutions, processes and management methods. In an interoperable information environment, a synergistic effect of interaction is achieved, in which each participant benefits from the use of data and increases the efficiency of their activities. Interoperability is necessary to create a single barrier-free information environment based on the principles of openness, transparency, reusability, technological neutrality, user-centricity, information security and privacy. The article reveals the principles of interoperability applicable to the field of e-Health with reference to the experience of the European Union where the concept of interoperability has been most developed. Each of the principles is examined through the prism of legal issues that need to be taken into account during their implementation. Particular attention is paid to standardization, information security requirements (including the security of medical devices and applications), conflict resolution between the principle of long-term storage of data for reuse and legislation on personal data. The article points out the positive steps towards the regulatory and legal support of the interaction of health information systems in the Russian Federation. Thus, the Russian legislation provides the framework for development of the Unified state health information system (EGISZ). However, it stresses the fact that interoperability should not be isolated (intra-industry). Interoperability in a broad sense means openness of interaction with other information systems (intersectoral interaction), the architecture of which should also be built on similar universal standards. This purpose reasons the need to develop a unified strategy for interoperability in the Russian Federation. Such a strategy requires an integrated approach at the national level and participation of all stakeholders in its development and implementation.



Keywords

interoperability; data sharing; eHealth; telemedicine; information systems; standardization; information security.

Acknowledgements: The work is fulfilled as part of the Program of Fundamental Studies of the National Research University Higher School of Economics and with a subsidy as part of state support of the leading universities of Russia “5-100”.

For citation: Zhuravlev M.S. (2019) Interoperability as a Factor of Law Development in the Digital Economy (eHealth case). *Pravo. Zhurnal Vyshey shkoly ekonomiki*, no 3, pp. 98–116 (in Russian)

DOI: 10.17-323/2072-8166.2019.3.98.116



References

Ahlgren B., Hidell M., Ngai E. (2016) Internet of Things for Smart Cities: Interoperability and Open Data. *Internet Computing*, issue 6, pp. 52–56.

Bodiroga-Vukobrat N., Rukavina D., Pavelić K., Sander G. (2016) *Personalized Medicine. A New Medical and Social Challenge*. Berlin: Springer, 278 p.

Borodin M.V. (2016) On Concepts and Principles in the Sphere of Electronic Document Management. *Actualnye problemy rossiyskogo prava*, no 2, pp. 102–109 (in Russian)

Burleson W., Carrara S. (eds.) (2014) *Security and Privacy for Implantable Medical Devices*. Berlin: Springer, 205 p.

Craft R. (2005) Toward Technical Interoperability in Telemedicine. *Telemedicine and e-Health*, no 3, pp. 384–404.

Demetrius K. (2014) Privacy-Invasive Technologies and Privacy by Design: Safeguarding Privacy, Liberty and Security in the 21st Century. In: *Information Technology and Law Series*. Berlin: Springer, 338 p.

Drexler J. (2016) Designing Competitive Markets for Industrial Data: Between Propertisation and Access. *Max Planck Institute for Innovation & Competition Research Paper*, no 16, 70 p.

Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B. (2015) Review of current telemedicine applications for chronic diseases. Toward a more integrated system? *Innovation and Research in Bio Medical Engineering*, issue 3, pp. 133–157.

Finet P., Le Bouquin Jeannès R., Dameron O., Gibaud B. (2018) Interoperable Infrastructure and Implementation of a Health Data Model for Remote Monitoring of Chronic Diseases with Comorbidities. *Innovation and Research in Bio Medical Engineering*, issue 3, pp. 151–159.

Kamyshanskaya S.V. (2016) Open Software and Information Security of the Russian Federation. *Vlast' zakona*, no 3, pp. 87–95 (in Russian)

Marcheschi P. (2017) Relevance of eHealth Standards for Big Data Interoperability in Radiology and beyond. *La radiologia medica*, issue 6, pp. 437–443.

Oemig F., Snelick R. (2016) *Healthcare Interoperability Standards Compliance Handbook*. Berlin: Springer, 662 p.

Purtova N., Kosta E., Koops B. (2015) Laws and Regulations for Digital Health. In: Fricker S., Thümmler C., Gavras A. (eds.) *Requirements Engineering for Digital Health*. Dordrecht: Springer, pp. 47–74.

Talapina E.V. (2018) Legal Regulation of Digital Government in Russia: Possibility of OECD Requirements Implementation. *Gosudarstvennaya vlast' i mestnoe samoupravlenie*, no 3, pp. 20–25 (in Russian)

Tereschenko L.K. (2004) Services: State, Public, Social. *Zhurnal rossiyskogo prava*, no 10, pp. 15–23 (in Russian)