

НАУЧНАЯ СТАТЬЯ

УДК 342.7

Дата поступления: 13.02.2024

рецензирования: 16.03.2024

принятия: 20.06.2024

Владислава Э. Мамедова

Самарский национальный исследовательский университет имени академика С.П. Королева, г. Самара, Российская Федерация; Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, г. Москва, Российская Федерация

Риск-ориентированный подход как методологическая основа публично-правового регулирования гарантий защиты персонифицированной медицинской информации

Аннотация: Статья посвящена проблемам обеспечения эффективного функционирования режима защиты персонифицированной медицинской информации пациентов в контексте развития и внедрения информационных технологий в медицинскую деятельность. В качестве теоретической основы автор использовал концепт «врачебная тайна», посредством формально-юридического метода научного познания установил соотношение и взаимосвязь указанного концепта с понятиями «персонифицированный учет», «персонифицированная медицинская информация» и сделал вывод о необходимости распространения режима защиты врачебной тайны на все данные, подлежащие персонифицированному медицинскому учету. Отметил, что наряду с преимуществами, возникающими при применении информационных технологий субъекты медицинских правоотношений сталкиваются с новыми рисками. На основании использования методов анализа, синтеза и классификации выделил три основных риска: неправомерный доступ к персонифицированной медицинской информации; ее незаконное использование и распространение; искажение объективной персонифицированной медицинской информации. При этом сделал вывод, что указанные риски обусловлены как человеческим, так и техническим факторами. Чрезмерное вмешательство в медицинские правоотношения может негативно сказаться на развитии указанной отрасли, что обуславливает необходимость разработки такой методологической основы к правовому регулированию, которая бы позволяла точно, но при этом системно нивелировать риски нарушения информационных прав граждан в рамках медицинской деятельности. В качестве такой основы автор предлагает использовать риск-ориентированный подход, основанный на приоритизации рисков. Используя указанный подход, автор провел ранжирование рисков и представил программу возможного правового регулирования исследуемой сферы, направленную на их последовательное предотвращение.

Ключевые слова: информационные права; информационные технологии; информационная система; медицинская помощь; защита персональных данных; личная тайна; врачебная тайна; персонифицированная медицинская информация; персонифицированный медицинский учет.

Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

Благодарности: Исследование выполнено при финансовой поддержке РНФ в рамках научного проекта «Концептуализация системы гарантий защиты персонифицированной информации человека при проведении медицинской диагностики и исследований» № 24-28-00794.

Цитирование: Мамедова, Владислава Э. 2024. «Риск-ориентированный подход как методологическая основа публично-правового регулирования гарантий защиты персонифицированной медицинской информации». *Юридический аналитический журнал Juridical Analytical Journal* 19 (1): 39–46. <http://doi.org/10.18287/1810-4088-2024-19-1-39-46>.

ИНФОРМАЦИЯ ОБ АВТОРЕ

© Владислава Э. Мамедова, 2024

Владислава Эдуардовна Мамедова, кандидат юридических наук, доцент, кафедра государственного и административного права, Самарский национальный исследовательский университет имени академика С.П. Королева, 443086, Российская Федерация, г. Самара, Московское шоссе, 34; старший научный сотрудник, отдел конституционного права, Институт законодательства и сравнительного правоведения при Правительстве Российской Федерации, 117218, Российская Федерация, г. Москва, ул. Б. Черемушкинская, 34.

e-mail: vladislava0804@mail.ru

SCIENTIFIC ARTICLE

Submitted: 13.02.2024
Revised: 16.03.2024
Accepted: 20.06.2024

Vladislava E. Mamedova Samara National Research University, Samara, Russian Federation;
The Institute of Legislation and Comparative Law under the Government
of the Russian Federation, Moscow, Russian Federation

Risk-based approach as a methodological basis for public legal regulation of guarantees for the protection of personalized medical information

Abstract: The article deals with the problems of ensuring the effective functioning of the regime for protecting personalized medical information of patients in the context of the development and implementation of information technologies in medical activities. As a theoretical basis, the author used the concept of “medical confidentiality”, through the formal legal method of scientific knowledge, established the relationship and interconnection of this concept with the concepts of “personalized accounting”, “personalized medical information” and concluded that it is necessary to extend the regime of protection of medical confidentiality to all data, subject to personalized medical registration. The author notes that along with the advantages arising from the use of information technologies, subjects of medical legal relations face new risks. Based on the use of methods of analysis, synthesis and classification, the author identified three main risks: unauthorized access to personalized medical information; its illegal use and distribution; distortion of objective personalized medical information. It was concluded that these risks are caused by both human and technical factors. The author points out that excessive interference in medical legal relations can negatively affect the development of this industry, which necessitates the development of a methodological basis for legal regulation that would allow targeted, but at the same time systematically leveling the risks of violation of the information rights of citizens within the framework of medical activities. As such a basis, the author proposes to use a risk-oriented approach based on risk prioritization. Using this approach, the author ranked the risks and presented a program for possible legal regulation of the area under study, aimed at their consistent prevention.

Key words: information rights; information technology; information system; health care; protection of personal information; personal secret; medical secrecy; personalized medical information; personalized medical records.

Conflicts of interest: the author declared is no conflict of interest.

Acknowledgement: The study was carried out with the financial support of the Russian Science Foundation within the framework of the scientific project «Conceptualization of the system of guarantees for the protection of personalized human information during medical diagnostics and research» № 24-28-00794.

Citation: Mamedova, Vladislava E. “Risk-based approach as a methodological basis for public legal regulation of guarantees for the protection of personalized medical information”. *Juridicheskii analiticheskii zhurnal Juridical Analytical Journal* 19 (1): 39–46. <http://doi.org/10.18287/1810-4088-2024-19-1-39-46>. (In Russian)

INFORMATION ABOUT THE AUTHOR

© Vladislava E. Mamedova, 2024

Vladislava E. Mamedova, Candidate of Legal Sciences, associate professor, Department of State and Administrative Law, Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russian Federation; scientific employee of the Department of Constitutional Law, The Institute of Legislation and Comparative Law under the Government of the Russian Federation, 34, B. Chermushkinskaya Street, Moscow, 117218, Russian Federation.

e-mail: vladislava0804@mail.ru

Введение

Масштабное внедрение электронного документооборота, информационных баз и систем является во многом неизбежным и необходимым этапом развития системы здравоохранения не только в Российской Федерации, но и во всем мире. Очевидно, что

такие технологии оптимизируют процессы при предоставлении медицинской помощи и способствуют эффективному использованию ресурсов.

В то же время широкое распространение информационных технологий в медицине ставит человечество перед многими вызовами и риска-

ми, которые в целом можно подразделить на две группы, связанные:

1) с необходимостью обеспечения должного качества медицинской помощи, оказываемой с использованием информационных технологий;

2) с обязательностью соблюдения высоких требований к защите персонифицированной медицинской информации.

В предмет настоящей статьи входят риски, включенные во вторую группу. Развитие медицины, биологии и информационных технологий приводит к появлению новых видов информации, например генетической, биометрической, персонифицированной медицинской и т. д. (Волков 2022, 69; Крюкова, Инюшкин 2023, 29–34; Инюшкин 2023, 28–31). Использование такой информации без согласия ее субъекта может привести к нарушению прав гражданина в широком спектре правоотношений: миграционных, страховых, банковских и других. В этой связи защите всех видов медицинской информации должно уделяться пристальное внимание ученых-юристов.

К вопросу о соотношении понятий «врачебная тайна» и «персонифицированная медицинская информация»

Статья 92 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»¹ (далее – Федеральный закон № 323-ФЗ) закрепляет порядок ведения персонифицированного учета в сфере здравоохранения, при этом сведения, подлежащие учету, классифицируются по субъекту: о лицах, которые участвуют в осуществлении медицинской и фармацевтической деятельности; обучающихся по медицинским и фармацевтическим образовательным программам; лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования (далее – пациенты).

Последняя группа сведений включает как «анкетные» данные пациентов (ФИО, дата и место рождения и т. д.), так и собственно медицинскую информацию (анамнез, диагноз, сведения об оказанной медицинской помощи). Очевидно, что такая информация подлежит защите в рамках режима, установленного Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»². В то же время,

статья 13 Федерального закона № 323-ФЗ устанавливает особый режим защиты врачебной тайны, которая включает в себя сведения как медицинского (состояние здоровья, диагноз, иные сведения, полученные при его медицинском обследовании и лечении), так и немедицинского характера (о факте обращения гражданина за оказанием медицинской помощи).

Стоит отметить, что законодатель не устанавливает соотношения сведений пациента, подлежащих персонифицированному учету, и данных, составляющих врачебную тайну. Дискуссионным данный вопрос является и для ученых-юристов (Подузова 2023, 86–92; Бойко, Бузина 2021, 37–42; Корнеева 2015, 42–45). Полагаем, что отнесение персонифицированной информации медицинского характера к врачебной тайне не должно подвергаться сомнениям. При этом суждение о том, что сведения немедицинского характера, подлежащие персонифицированному учету, не составляют врачебной тайны, на первый взгляд представляется обоснованным в силу значительных отличий их текстуального закрепления. Однако при анализе содержания указанных понятий следует учитывать цель их закрепления и подход, избранный законодателем при их конструировании.

Сведения, подлежащие персонифицированному учету, закрепляются главой 12 Федерального закона № 323-ФЗ, посвященной организации контроля в сфере охраны здоровья, и служат утилитарным целям – созданию и функционирования систем информационного обеспечения здравоохранения. В основе текстуальной фиксации содержания указанных сведений лежит структурный подход, ставящий целью закрепление их исчерпывающего перечня, необходимого для информационного обеспечения деятельности системы здравоохранения.

В свою очередь, в основе определения понятия врачебной тайны использован сущностный подход, позволяющий выделить конститутивные признаки сведений, составляющих ее содержание. Одним из таких признаков выступает связь сведений с фактом обращения гражданина за оказанием медицинской помощи. Полагаем, что, поскольку включение данных пациента в систему персонифицированного учета, по сути, выступает свидетельством обращения гражданина в медицинскую организацию, режим врачебной тайны следует распространять на все данные, подлежащие персонифицированному медицинскому учету. Такой расширительный подход, вопреки возможному

¹ Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». 2011. *Собрание законодательства РФ* 48. Ст. 6724.

² Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». 2006. *Собрание законодательства Российской Федерации* 31 (ч. 1). Ст. 3451.

возражению о чрезмерности возлагаемых на лиц, имеющих доступ к персонифицированной медицинской информации, обязательств, наоборот, исключит необходимость обеспечения функционирования двухкомпонентной системы защиты данных: персональных и составляющих врачебную тайну, тем самым снизит организационные издержки. Кроме того, предлагаемый подход исключит ошибки в квалификации тех или иных данных в качестве составляющих врачебную тайну и предотвратит риск установления ненадлежащего режима защиты в отношении них.

Риск-ориентированный подход к защите персонифицированной медицинской информации

При моделировании системы гарантий защиты персонифицированной медицинской информации следует исходить из ряда положений. Во-первых, изменения, вносимые в систему нормативного регулирования, не должны приводить к формированию множественности нормативных правовых актов и необоснованному усложнению их текстуального содержания. Данное требование, в частности, обусловлено тем, что адресатами указанных норм выступают лица, не обладающие специальными юридическими знаниями, а именно работники медицинских организаций, операторов информационных систем и т. д. Во-вторых, закрепляемые законодательством гарантии защиты персонифицированной медицинской информации не должны налагать чрезмерные обязанности на участников правоотношений, в частности медицинских работников. Непропорциональный объем обязанностей может препятствовать развитию как системы здравоохранения, так и медицинской науки в целом, поскольку лишит субъектов указанной деятельности необходимой степени свободы. В-третьих, при формировании системы гарантий защиты персонифицированной информации следует учитывать реально существующие риски нарушения установленного режима ее защиты и не допускать формирования т. н. «опережающего» регулирования в отношении потенциальных нарушений, поскольку такой подход также может негативно отразиться на развитии медицины в целом.

Резюмируя указанное выше, полагаем целесообразным использовать риск-ориентированный подход в качестве методологической основы институционализации системы гарантий защиты персонифицированной медицинской информации. Риск-ориентированный подход

в контексте применения к рассматриваемой сфере предполагает закрепление более детализированного нормативного регулирования по отношению к тем аспектам общественных отношений, которые связаны с наибольшими рисками нарушения режима защиты персонифицированной медицинской информации. В случае отсутствия таких рисков установление дополнительного регулирования не требуется.

Таким образом, в рамках риск-ориентированного подхода следует выявить риски нарушения режима защиты персонифицированной медицинской информации при взаимодействии с ней и провести их приоритизацию на основе оценки распространенности и степени тяжести последствий их реализации.

Обобщая данные медицинских организаций, судебную практику и научную литературу (Лазарев, Гаджиев 2020; Антонова, Бальхаева, Гаунова и др. 2019), можно выделить несколько укрупненных видов рисков в исследуемой сфере:

- 1) неправомерный доступ к персонифицированной медицинской информации;
- 2) ее незаконное использование и распространение;
- 3) искажение объективной персонифицированной медицинской информации.

Иные риски с той или иной степенью условности можно отнести к трем указанным выше.

Отметим, что указанные риски обусловлены двумя факторами: техническим и человеческим.

Технический фактор включает:

- а) неисправности, сбои и ошибки в функционировании медицинских информационных систем, специальных технических средств и каналов передачи данных;

- б) повреждение и утрату носителей информации;

- в) использование в работе информационных систем протоколов шифрования каналов передачи данных (например, SSL-шифрование), не соответствующих требованиям к классу защищенности информации второго класса (K2)³;

- г) нарушение требований по размещению используемых серверов в выделенном защищенном сегменте центра обработки данных, а также использование зарубежных серверов и ИТ-инфраструктуры (в т. ч. расположенных в недружественных странах) (Kolosova 2021, 7; Липчанская, Заметина 2020, 89; Абдуллаев, Абрамова, Абызова и др. 2023, 292–305).

³ См.: Пункт 4 приложения 1 к Приказу ФСТЭК России от 11.02.2013 № 17 “Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах”. 2013. *Российская газета* 136.

Так называемый технический фактор является относительно новым вызовом для системы защиты медицинской информации. При этом использование информационных технологий в медицине выступает своего рода катализатором указанных выше рисков: возможности для злоупотреблений в сфере доступа и использования медицинской информации многократно возрастают. Этот факт следует учитывать при приоритизации рисков.

Человеческий фактор включает в себя неправомерные действия (умышленные и неосторожные) субъектов правоотношений. Указанные субъекты могут быть представлены участниками общественных отношений по оказанию медицинской помощи: работниками медицинской организации; оператором персональных данных, в т. ч. оператором медицинских информационных систем; пациентами (нарушение правил обработки персональных данных, требований информационной безопасности, в т. ч. передача доступа к учетной записи, усиленной квалифицированной электронной подписи (далее – УКЭП) третьим лицам; нарушение правил эксплуатации информационных систем; подлог и умышленное искажение данных и т. д.).

Кроме того, недобросовестные действия, нарушающие режим защиты персонифицированной медицинской информации, могут быть совершены третьими лицами (например, в рамках хакерских атак, мошеннических действий и т. д.).

В литературе встречается классификация рисков на «объективные события, независимые от воли человека, и события, представляющие собой причинение вреда в результате деятельности человека» (Михайлова 2022, 42), то есть с точки зрения теории права на события и действия как виды юридических фактов. В целом эта классификация во многом пересекается с представленной нами выше и так же имеет важное значение для выявления и первичной систематизации существующих в исследуемой сфере рисков, т. е. служит цели постановки проблемы, но не ее решения. Данный тезис вытекает из следующих положений.

Во-первых, разделение на технический и человеческий фактор является условным, поскольку, как правило, нарушения в сфере оборота персонифицированной медицинской информации при применении телемедицинских технологий обусловлены комплексом причин. Так, сбой в работе технических средств может затруднить доступ к медицинской информации,

но при отсутствии недобросовестных действий со стороны тех или иных субъектов такой сбой не тождествен автоматической утечке персонифицированных данных пациентов. И, наоборот, прямой умысел на неправомерное завладение персонифицированной медицинской информацией практически сложно реализовать в отсутствие технических недостатков функционирования соответствующих информационных систем.

Во-вторых, право не способно оказывать регулятивное воздействие на события, в связи с чем его предметом являются общественные отношения, возникающие вследствие того или иного юридического факта, которым может выступить событие. Технические средства и информационные платформы являются искусственно созданными системами, поэтому недостатки и сбои в их функционировании в той или иной степени являются следствием умышленных либо неосторожных действий граждан. Признание таких сбоев абсолютными событиями означает снижение уровня ответственности разработчиков и операторов соответствующих средств и систем, что в сфере обработки информации, в отношении которой установлен особый режим охраны (личная и врачебная тайна), представляется недопустимым (Кибальник, Волосюк 2018, 176; Крюкова, Инюшкин 2023, 33).

Перейдем к приоритизации выявленных выше рисков. При системном анализе выявленных рисков становится очевидным, что риск незаконного использования и распространения персонифицированной медицинской информации является производным от риска неправомерного доступа к ней. В связи с этим будет логичным рассматривать необходимость предотвращения неправомерного доступа к медицинской информации в качестве первоочередной. Как было отмечено выше, применение информационных технологий многократно увеличивает риски неправомерного доступа к защищаемой информации. При этом основные участники правоотношений – медицинские организации, их работники и пациенты – не обладают необходимым уровнем специальных знаний и технических возможностей, позволявших бы в полной мере минимизировать обозначенные риски. В связи с этим приоритетным должно выступать регулирование, направленное на минимизацию рисков неправомерного доступа к медицинской информации, обусловленных техническим фактором. Бремя их предотвращения должно ложиться на субъекта, обладающего необходимыми знаниями, техническими

и организационными ресурсами. В рассматриваемых отношениях таким субъектом выступает оператор медицинской информационной системы, чей статус в настоящее время представляется недостаточно конкретизированным законодательством.

При условии минимизации указанного риска вторым по приоритету выступает обусловленный человеческим фактором риск неправомерного доступа к информации, который, как правило, связан с возможностью физического доступа к носителям такой информации. Ответственными субъектами за предотвращение такого риска в первую очередь следует считать медицинские организации и их работников. В целом весь предыдущий период развития законодательства о врачебной тайне был преимущественно направлен на минимизацию данной категории риска, в связи с чем общий уровень защищенности прав граждан в указанном контексте следует считать удовлетворительным. При этом полагаем, что приоритетным способом воздействия на общественные отношения здесь должно выступать не столько новое нормативное регулирование, сколько дополнительное обучение медицинских работников, направленное на восприятие ими всего комплекса как деонтологических, так и правовых и технических требований, направленных на всестороннюю защиту прав пациентов.

Взаимосвязанный с неправомерным доступом к информации риск – риск ее незаконного использования и распространения – является следующим по приоритетности. Именно с ним могут быть связаны многочисленные нарушения прав гражданина в рамках правоотношений различной отраслевой направленности. Поскольку действия, направленные на предотвращение технических причин неправомерного доступа к информации, во многом предотвращают ее распространение и использование, приоритетным для данного риска считаем предотвращение т. н. человеческого фактора. Помимо обозначенных выше субъектов, здесь необходимо конкретизировать обязанности тех

субъектов, при взаимодействии с которыми используется соответствующая информация (страховые, кредитные организации, государственные и муниципальные органы и т. д.), в целях ее дополнительной верификации.

В рамках этого же риска необходимо совершенствовать нормы о юридической ответственности лиц, виновных в совершении деяний, направленных на использование и распространение персонифицированной медицинской информации, как основной способ правового воздействия на них.

Искажения объективной персонифицированной медицинской информации, в первую очередь влияют на правоотношения в сфере медицины и в большинстве своем могут быть исправлены в ходе перепроверки данных, поэтому этот риск мы рассматриваем в качестве менее приоритетного для правового регулирования.

Недопустимо не учитывать тот факт, что пациенты также могут как умышленно, так и непреднамеренно способствовать нарушениям своих информационных прав в сфере медицины. Риски, связанные с действиями пациентов, следует предотвращать посредством общего правового просвещения.

Заключение

Таким образом, особая значимость персонифицированной медицинской информации требует системного подхода к закреплению системы правовых гарантий ее защиты. В качестве основы построения такой системы допустимо использовать риск-ориентированный подход, предполагающий наиболее детальное регулирование тех сфер общественных отношений, в которых риски нарушения информационных прав пациентов наиболее распространены. Приоритизация основных рисков позволяет выстроить программу формирования необходимого правового регулирования, направленную на последовательное предотвращение рисков неправомерного доступа к персонифицированной медицинской информации, ее незаконного использования и распространения, а также ис-

Библиография

Абдуллаев, Казбек А., Анастасия В. Абрамова и др. 2023. *Конвергенция частноправового регулирования общественных отношений сквозь призму эффективности права*: монография. Москва: Юстицинформ: 672 с. <https://znanium.ru/catalog/document?id=444103&ysclid=lyclh2i5w2797216429>.

Антонова, Наталья В., Саяна Б. Бальхаева и др. 2019. *Юридическая концепция роботизации*: монография. Москва: Проспект: 238 с. <https://znanium.ru/catalog/document?id=388968&ysclid=lyclq4j5z8358079355>.

кажбойко, Игорь Б., Ольга И. Бузина. 2021. “О врачебной тайне и ее соблюдении в Федеральном законе от 21 ноября 2011 г. № 323-ФЗ “Об основах охраны здоровья граждан в Российской Федерации””. *Медицинское право* 3: 37–42. <https://www.elibrary.ru/item.asp?id=46235655>, <https://www.elibrary.ru/yknngp>.

Волков, Владислав Э. 2022. *Цифровое право. Общая часть: учебное пособие*. Самара: Издательство Самарского университета. <https://digilaw.ru/wp-content/uploads/2022/10/volkov-v.e.-czifrovoe-pravo.-obshhaya-chast.pdf?ysclid=lycu8e2qt8585781956>.

Защита данных: научно-практический комментарий к судебной практике. 2020. Отв. ред. В.В. Лазарев, Х.И. Гаджиев. Москва: ИЗиСП; Контракт: 176 с. https://izak.ru/upload/iblock/3d6/Zashchita-dannykh_Nauchno_prakticheskiy-kommentariy-k-sudebnoy-praktike_Blok.pdf?ysclid=lycq82rel4984954267.

Инюшкин, Андрей А. 2023. “Особенности генетической информации, как объекта правовой охраны”. *Правовая основа социально-экономических отношений в аспекте вызовов современности: сборник научных статей I Всероссийской с международным участием междисциплинарной научно-практической конференции*. Самара: Исакова Т.С. (БИЮР): 28–31. <https://www.elibrary.ru/item.asp?id=59932879>. EDN: <https://www.elibrary.ru/gywjjm>.

Кибальник, Алексей Г., Павел В. Волосюк. 2018. “Искусственный интеллект: вопросы уголовно-правовой доктрины, ожидающие ответов”. *Юридическая наука и практика: Вестник Нижегородской академии МВД России* 4 (44): 173–178. <http://doi.org/10.24411/2078-5356-2018-10428>.

Корнеева, Ольга И. 2015. “Взгляд на персонифицированный учет при осуществлении медицинской деятельности с позиций врачебной тайны”. *Медицинское право* 5: 42–45. <https://www.elibrary.ru/item.asp?id=23925531>, <https://www.elibrary.ru/udopzh>.

Крюкова, Елена С., Андрей А. Инюшкин. 2023. “Интеллектуальные системы и персонализированная медицина: проблемы правового регулирования”. *Юрист* 9: 29–34. <https://doi.org/10.18572/1812-3929-2023-9-29-34>.

Липчанская, Мария А., Тамара В. Заметина. 2020. “Социальные права граждан в условиях использования искусственного интеллекта: правовые основы и пробелы законодательного регулирования в России”. *Журнал российского права* 11: 78–96. <http://doi.org/10.12737/jrl.2020.134>.

Михайлова, Анастасия С. 2022. “К вопросу о телемедицине и не только”. *Медицинское право* 4: 38–44. <https://www.elibrary.ru/item.asp?id=49378816>, <https://www.elibrary.ru/kbjpoo>.

Подузова, Екатерина Б. 2023. “Персональные данные пациента и его законного представителя: специфика электронного предоставления в контексте применения технологий “искусственного интеллекта” в digital-медицине”. *Актуальные проблемы российского права* 4: 86–92. <http://doi.org/10.17803/1994-1471.2023.149.4.086-092>.

References

Abdullaev, Kazbek A., Anastasia V. Abramova et al. 2023. *Convergence of private law regulation of public relations through the prism of the effectiveness of law: monograph*. Moscow: Iustitsinform: 672 p. <https://znanium.ru/catalog/document?id=444103&ysclid=lychl2i5w2797216429>. (In Russian)

Antonova, Natalia V., Sayana B. Balkhaeva et al. 2019. *The legal concept of robotization: monograph*. Moscow: Prospekt: 238 p. <https://znanium.ru/catalog/document?id=388968&ysclid=lyclq4j5z8358079355>. (In Russian)

Boyko, Igor B., Buzina, Olga I. 2021. “On medical secrecy and its observance in the Federal Law No. 323-FZ “On the Fundamentals of Health Protection of Citizens in the Russian Federation” dated November 21, 2011, No. 323-FZ”. *Medical Law* 3: 37–42. <https://www.elibrary.ru/item.asp?id=46235655>, <https://www.elibrary.ru/yknngp>. (In Russian)

Inyushkin, Andrey A. 2023. “Peculiarities of genetic information as an object of legal protection”. In: *Legal basis of socio-economic relations in the aspect of modern challenges: collection of scientific articles of the First All-Russian interdisciplinary research and practical conference with international participation*. Samara: Isakova T.S. (BIYuR): 28–31. <https://www.elibrary.ru/item.asp?id=59932879>. EDN: <https://www.elibrary.ru/gywjjm>. (In Russian)

Kibalnik, Alexei G., Pavel V. Volosyuk. 2018. “Artificial intelligence: doctrinal criminal law questions awaiting answers”. *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia* 4 (44): 173–178. <http://doi.org/10.24411/2078-5356-2018-10428>. (In Russian)

Korneeva, Olga I. 2015. “Patient-specific records in medical activities from the viewpoint of medical secrecy”. *Medical Law* 5: 42–45. <https://www.elibrary.ru/item.asp?id=23925531>, <https://www.elibrary.ru/udopzh>. (In Russian)

Kryukova, Elena S., Andrey A. Inyushkin. 2023. “Intelligent systems and personalized medicine: problems of legal regulation”. *Jurist* 9: 29–34. <https://doi.org/10.18572/1812-3929-2023-9-29-34>. (In Russian)

Lazarev V.V., Gadzhiev H.I. (Eds.) 2020. Data protection: scientific and practical commentary on judicial practice. Moscow: IZiSP; Kontrakt: 176 p. https://izak.ru/upload/iblock/3d6/Zashchita-dannykh_Nauchno_prakticheskiy-kommentariy-k-sudebnoy-praktike_Blok.pdf?ysclid=lycq82rel4984954267. (In Russian)

Lipchanskaya, Maria A., Tamara V. Zametina. 2020. “Social Rights of Citizens Using Artificial Intelligence: Legal Bases and Gaps in Legislative Regulation in Russia”. *Journal of Russian Law* 11: 78–96. <http://doi.org/10.12737/jrl.2020.134>. (In Russian)

Mikhailova, Anastasia S. 2022. “On telemedicine and much more”. *Medical Law* 4: 38–44. <https://www.elibrary.ru/item.asp?id=49378816>. EDN: <https://www.elibrary.ru/kbjpoo>. (In Russian)

Poduzova, Ekaterina B. 2023. “Personal Data of the Patient and His Legal Representative: The Specifics of Electronic Provision in the context of the Use of «Artificial Intelligence» Technologies in Digital Medicine”. *Actual Problems of Russian Law* 4: 86–92. <http://doi.org/10.17803/1994-1471.2023.149.4.086-092>. (In Russian)

Volkov, Vladislav E. 2022. *Digital law. The general part: textbook*. Samara: Izdatel'stvo Samarskogo universiteta. <https://digilaw.ru/wp-content/uploads/2022/10/volkov-v.e.-czifrovoe-pravo.-obshhaya-chast.pdf?ysclid=lycu8e2qt8585781956>. (In Russian)