Научная статья
УДК 347.1:654:004.8
EDN: https://elibrary.ru/vskcfb
DOI: https://doi.org/10.21202/jdtl.2023.13

Правовые аспекты использования искусственного интеллекта в телемедицине

Кьяра Галлезе-Нобиле

Эйндховенский технологический университет
г. Эйндховен, Королевство Нидерландов;
Университет Триеста
г. Триест, Итальянская Республика

Ключевые слова

Законодательство,
защита данных,
искусственный интеллект,
персональные данные,
право,
регулирование,
телемедицина,
цифровое неравенство,
цифровые технологии,
частная жизнь

Аннотация

Цель: стремительное распространение телемедицины в клинической практике и возрастающая роль искусственного интеллекта ставят перед юристами множество проблем относительно охраны неприкосновенности частной жизни. Повышенная сензитивность данных в этой области заставляет уделить особое внимание правовым аспектам таких систем. В статье исследуются правовые последствия использования искусственного интеллекта в телемедицине, в частности, систем непрерывного обучения и автоматизированного принятия решений; фактически оказание персонализированных медицинских услуг через системы непрерывного обучения может представлять дополнительный риск. Особого внимания заслуживают уязвимые группы населения – дети, пожилые люди и тяжелобольные пациенты – как по причине цифрового неравенства, так и из-за сложностей с выражением своего согласия.

Методы: сравнительно-правовые и формально-правовые методы исследования позволили проанализировать текущее состояние регулирования искусственного интеллекта и выявить его соотношение с нормами регулирования телемедицины, Общим регламентом ЕС по защите персональных данных и другими нормами.

Результаты: изучены правовые последствия использования искусственного интеллекта в телемедицине, в частности, систем непрерывного обучения и автоматизированного принятия решений; автор приходит к выводу, что оказание персонализированных медицинских услуг через системы непрерывного обучения представляет дополнительные риски, и предлагает пути их минимизации. Автор также уделяет особое внимание вопросам информированного согласия уязвимых групп населения (детей, пожилых, тяжелобольных).

Научная новизна: изучены актуальные риски и проблемы, возникающие в сфере использования искусственного интеллекта в телемедицине, при этом особое внимание уделено системам непрерывного обучения.

Практическая значимость: полученные результаты восполняют недостаток научных исследований по данной теме, могут быть использованы в законодательном процессе в сфере использования искусственного интеллекта в телемедицине, а также в качестве основы для будущих исследований в данной области.

Для цитирования

Галлезе-Нобиле, К. (2023). Правовые аспекты использования искусственного интеллекта в телемедицине. *Journal of Digital Technologies and Law*, *1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

Содержание

Введение
1. Нормативно-правовая база телемедицины в Европе
2. Искусственный интеллект в телемедицине
3. Непрерывное обучение и персонализированная медицина
4. Вопросы охраны частной жизни в телемедицине
5. Статья 22 Общего регламента ЕС по защите персональных данных и контроль со стороны человека
6. Информированное согласие
7. Уязвимые группы
8. Баланс между охраной неприкосновенности частной жизни и защитой от вреда при дистанционной работе
9. Меры дополнительной защиты в форме аудита искусственного интеллекта
Заключение
Список литературы

Введение

Термин «телемедицина» был предложен в 1970-е гг. Томасом Бёрдом (Thomas Bird); Strehle и Shabde определили его как «лечение на расстоянии» (Strehle & Shabde, 2006). С течением времени появилось несколько официальных определений, например: «предоставление услуг здравоохранения, путем использования ИКТ, в ситуациях, когда специалист в области здравоохранения и пациент (или два специалиста в области здравоохранения) не находятся в одном месте. Телемедицина включает в себя безопасную передачу медицинских данных и информации в форме текста, звуков, изображений и других форм, необходимой профилактики, диагностирования, лечения и последующего ведения пациентов. Телемедицина охватывает широкий спектр услуг. Наиболее часто упоминаемыми из них в рецензируемых обзорах являются телерадиология, телепатология, теледерматология, телеконсультирование, теленаблюдение, телехирургия и телеофтальмология. Другие возможные услуги включают

колл-центры/информационные центры онлайн для пациентов, удаленные консультации/электронные приемы или видеоконференции специалистов.

Информационные порталы, электронные системы ведения медицинских карт, электронная передача рецептов и назначений (е-рецепты, е-назначения) не рассматриваются как услуги телемедицины для целей данного Сообщения[1], которое стало основой для государственного регулирования (например, для определения, сформулированного министерством Италии в 2012 г.)[2].

Новый метод предоставления медицинских услуг не только способствует оптимизации и повышению эффективности данных процессов, при этом не заменяя традиционную очную медицину (Burrai et al., 2021), но и лучше организует последующее ведение пациента и профилактические мероприятия; он более удобен, особенно для маломобильных и тяжелых пациентов. Фактически по сравнению с традиционной медициной устройства, используемые для наблюдения за пациентом в домашних условиях, позволяют им реже ездить в больницу, с комфортом оставаться дома (или, например, в гостинице, если они заболели на отдыхе или в деловой поездке). Это особенно важно во время пандемии, так как снижает вероятность распространения инфекции или заражения в медицинском учреждении. Можно отметить, что именно ситуация с вирусом Covid-19 способствовала развитию телемедицины, так как она дала возможность получить медицинскую помощь даже в условиях ограничений на передвижение.

При этом такая уникальная возможность несет в себе определенные риски и поднимает множество различных правовых вопросов. В настоящей статье мы фокусируемся на правовых вопросах, связанных с использованием искусственного интеллекта (далее – ИИ) в телемедицине, и в частности систем непрерывного обучения.

1. Нормативно-правовая база телемедицины в Европе

Стремительное распространение телемедицины в клинической практике некоторое время назад заставило Евросоюз изучить последствия использования новых технологий для пациентов, развития рынка электронного здравоохранения, создания общеевропейского пространства данных о здоровье, а также возможного влияния всех этих факторов на сферу здравоохранения в странах-членах ЕС. В этой связи в течение нескольких лет были выпущены ряд инструментов «мягкого права», такие как руководства, рекомендации и другие инструменты. Они подробно проанализированы в работе Botrugno (Bortugno, 2014). Кроме того, Регламент Евросоюза о медицинских устройствах, вступивший в силу 26 мая 2021 г., относится ко всем телемедицинским устройствам, используемым для постановки диагноза и оказания помощи на расстоянии[3]. В Италии данная сфера также в основном регулируется мяг-

1 Сообщение Комиссии Европейскому Парламенту, Совету, Европейскому экономическому и социальному комитету и Комитету регионов о телемедицине на благо пациентов, систем здравоохранения и общества в целом, 2008. https://commission.europa.eu/system/files/2022-10/cwp_2023.pdf

2 Ministero della Salute. Telemedicina – Linee di indirizzo nazionali, 2012. https://www.salute.gov.it/portale/documentazione/p6_2_2_1.jsp?id=2129

3 Regulation (Eu) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745

ким правом, в частности, Руководством от 2012 г.[4] Кроме того, в 2017 г. был принят Закон № 219, регулирующий вопросы информированного согласия и Распоряжения об ожидаемом обращении на случай возможной недееспособности. Как будет показано ниже, данная сфера приобретает особую важность в случае использования телемедицины через интеллектуальные системы. Исследователи отмечают, что если рассматривать эмоциональные потребности пациента как неотъемлемую часть терапии, то телемедицину следует считать услугой, встроенной в традиционные схемы (Campagna, 2020).

Как показано в работе Campagna, существующая нормативно-правовая база будет в ближайшее время дополнена новым европейским законом об ИИ, одобренным Еврокомиссией в 2021 г. (Campagna, 2020). Он предусматривает изменения в статусе телемедицинских устройств на основе ИИ, налагая строгие требования на их использование в медицинской практике, клинических испытаниях и научных исследованиях. Фактически медицинские устройства классифицируются данным положением как «высокорисковые». Новый закон станет дополнением Общего регламента ЕС по защите персональных данных (GDPR) и Европейского регламента о медицинских изделиях (MDR), предусматривая дополнительные гарантии для пользователей (включая как пациентов, так и медицинский персонал).

2. Искусственный интеллект в телемедицине

По мере технологического прогресса многие технологии искусственного интеллекта начали применяться в телемедицине с целью улучшить ее результативность, поскольку в ряде областей (таких как распознавание образов) возможности ИИ уже превзошли возможности человека.

Однако специалисты в области здравоохранения по-прежнему остерегаются использовать эти технологии в клинической практике: исследования, проведенные в 2020 г. Лабораторией цифровых инноваций в здравоохранении Политехнического университета Милана по теме «Сопутствующая медицинская помощь в чрезвычайных ситуациях, связанных с Covid-19», показали, что лишь 9 % итальянских врачей использовали новые технологии до пандемии и только 6 % из них работают в учреждениях, где такие технологии были внедрены (или усилены) во время пандемии. При этом 60 % медиков считают, что технологии искусственного интеллекта могут сыграть ключевую роль в чрезвычайных ситуациях, 52 % – что они способствуют персонализации медицинского обслуживания, 51 % думают, что они повышают эффективность медицинского обслуживания, а 50 % – что помогают снизить вероятность медицинских ошибок. Схожие результаты были получены и в других странах, где также поднимались вопросы врачебной ответственности (Scheetz et al., 2021). Однако исследования показывают, что широкая общественность с огромным недоверием относится к использованию моделей ИИ в медицине (Castagno & Khalifa, 2020).

Тенденции развития использования искусственного интеллекта в телемедицине можно разделить на четыре группы: наблюдение за пациентами, информация о здоровье, помощь в диагностировании и анализ информации (Pacis et al., 2018).

[4] Ministero della Salute, Telemedicina – Linee di indirizzo nazionali. https://www.salute.gov.it/portale/ehealth/homeEHealth.jsp

Данные технологии наиболее часто используются в таких областях медицины, как лечение диабета, кардиология, офтальмология, онкология, эпидемиология, дерматология. Во время пандемии телемедицина использовалась, помимо прочего, для ведения пациентов, подозревавшихся в инфицировании, и для помощи по хроническим заболеваниям (Ye, 2020). Как правило, пациенты носили на себе съемные устройства, такие как смарт-часы или датчики, или пользовались приложением для планшета; но также использовались и более инвазивные методы, например, пациент мог глотать капсулы, в доме могли устанавливаться камеры или использовались датчики для контроля действий, например, открывания упаковки с лекарством. Также применялись малоинвазивные методы, такие как использование приложения на смартфоне, особенно для молодых пациентов, которые могут приобщиться к телемедицине через игру (Giunti, 2014), и пожилых (Schatten & Protrka, 2021), которых необходимо стимулировать к знакомству с системами ИИ. Устройства с более сложными технологиями могут приспосабливаться к конкретному пациенту, продолжая обучаться во время использования. Это порождает ряд этических и правовых проблем, по которым доктрина и юридическая наука пытаются вести глубокий анализ, чтобы выработать руководящие принципы для исследователей и практиков в области здравоохранения, которые участвуют в разработке таких устройств. Фактически очень часто нормативное регулирование оказывается очень сложным даже для юристов, как это произошло в случае защиты персональных данных, что затрудняет эффективную защиту пациентов.

Комплексное нормативное регулирование осложняется также фрагментированностью сферы ИИ в рамках Евросоюза; исправить эту ситуацию призван новый проект закона об ИИ. На сегодняшний день, однако, сохраняются и сохранятся даже после вступления в силу этого закона многие особенности, характерные для отдельных стран – членов Евросоюза, касающиеся защиты персональных данных, профессиональной врачебной ответственности, информированного согласия, ответственности за качество продукции и уголовной ответственности.

3. Непрерывное обучение и персонализированная медицина

Одна из самых популярных моделей предоставления персонализированных медицинских услуг заключается в так называемом непрерывном обучении. Врачи стремятся предоставить пациентам наилучшие услуги, при этом в ряде случаев эти услуги необходимо привести в соответствие с потребностями конкретного пациента, которые различаются в зависимости от его этнической принадлежности, пола, привычек, семейного анамнеза, психологического состояния и т. д. Этой цели можно эффективно достичь с помощью ИИ, системы которого обучаются в процессе использования пациентом и приспосабливаются к характеристикам последнего с течением времени. С точки зрения права особого внимания заслуживают модели на основе машинного обучения (особенно глубокого обучения), а также модели на основе подхода «черный ящик» (Rodrigues, 2020; Lakkaraju, 2019), так как в этих случаях разработчики создают модель и предоставляют соответствующие образцы, но не знают конечного результата, потому что модель учится самостоятельно (перед выпуском на рынок, во время фазы обучения, а также после продажи). При этом часто невозможно узнать причин того или иного результата, выдаваемого моделями, поэтому важно исследовать и понимать, как они будут вести себя в рамках различных сценариев (Davis, 2016).

Эта проблема не ограничена телемедициной, но относится ко всем приложениям ИИ; однако использование такого типа моделей в контексте телемедицины ведет к крупным рискам – не только из-за типа используемых данных, но и из-за потенциального влияния на базовые права пациентов. Указанные системы могут представлять особую опасность в случае телемедицины, чем в случае очной медицины, поскольку пациент, пребывая в удалении, не находится под непосредственным наблюдением врача. Данную проблему мы рассмотрим ниже. Например, при мониторинге диабета у детей используются смарт-часы, измеряющие уровень сахара в крови, физиологические показатели (такие как сердечный ритм) напоминают о необходимости принимать пищу и двигаться, предлагают необходимый объем лекарства, который должен принять пациент, и передают результат врачу. На основании этого результата врач может назначить прием, анализы и медицинские исследования. В случае непрерывного обучения одна из ключевых проблем состоит в том, что ни разработчик, ни врач, который будет пользоваться системой ИИ, не знает заранее, как она будет себя вести и чему она обучится при взаимодействии с пациентом, поскольку эта система развивается во времени. Фактически следует принимать во внимание четыре аспекта. Во-первых, качество обучения отражает качество образцов: если пользователь предоставляет системе искаженные либо низкокачественные образцы, то поведение ИИ в конечном итоге изменится таким образом, чтобы соответствовать этим образцам.

Ярким примером является случай с чат-ботом Тэй[5]. В персонализированной телемедицине многие образцы предоставляются системе непосредственно пациентом. Очевидно, что пациент не специалист и зачастую не может понять последствий своего выбора. Например, ребенок может одолжить смарт-часы однокласснику или младшему брату, в результате чего в систему попадут неверные данные. Система решит, что уровень сахара в крови ребенка ниже, чем на самом деле, и порекомендует принять меньше лекарства. Даже если количество принимаемого лекарства контролируется врачом (что маловероятно в случае ежедневного приема лекарства, так как ежедневное наблюдение очень дорогостоящее), врач не поймет, что уровень глюкозы указан неверно из-за внешних факторов или из-за неправильного использования устройства пациентом, если только устройство не оснащено камерами наблюдения. В таких случаях единственным способом предотвратить неправильное использование устройства является теленаблюдение, что расценивается как вмешательство в частную жизнь и крайне нежелательно для пациента. Даже с точки зрения ответственности сложно определить, кто должен отвечать за ошибку системы в таких случаях. Должен ли производитель или разработчик нести ответственность за выпуск небезопасного устройства, не оснащенного механизмом наблюдения? Или врач за то, что не заметил ненормальные показатели крови? Родитель или опекун ребенка, не отследивший неправильное использование устройства? Для решения некоторых из этих вопросов 28 сентября 2022 г. Еврокомиссия опубликовала проект Директивы об ответственности ИИ, служащей дополнением к Закону ЕС об ИИ, в котором медицинские устройства рассматриваются как «высокорисковые системы»,

[5] Бот Тэй на основе искусственного интеллекта, принадлежащий компании Microsoft, стал расистским и нацистским. *The Guardian*. https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

а значит, должны соответствовать строгим требованиям. За необходимость подобного реформирования давно выступали ученые, поскольку существующие нормы ответственности не в состоянии регулировать использование систем ИИ, и в частности моделей машинного обучения (Gallese, 2022).

Новый проект устанавливает презумпцию ответственности лица, выпустившего систему на рынок: как правило, производитель или импортер должен будет нести ответственность за вред, причиненный системой, а «национальные суды должны признавать, с целью применения норм ответственности за вред, причинно-следственную связь между виной ответчика и результатами, произведенными системой ИИ, либо неспособностью системы ИИ произвести результат». Из этой новой нормы предусмотрены два исключения, в случае если заявитель может показать, что пользователь системы «не выполнил свои обязательства по использованию или наблюдению за системой ИИ в соответствии с прилагаемыми инструкциями по ее использованию или, в соответствующих случаях, приостановил или прервал ее использование согласно [Статье 29 Закона об ИИ]» либо «предоставил системе ИИ исходные данные, находящиеся под его контролем, которые не соответствовали предполагаемым задачам системы согласно [Статье 29(3) Закона об ИИ]». Данная норма направлена на защиту пользователей, поскольку сложно оценить причинно-следственную связь между поведением системы и неверным результатом (особенно в случае «черного ящика»).

В рамках данной нормы врачей сложно привлечь к ответственности как потому, что они не могут физически влиять на систему (если только им не предоставлены полный дистанционный контроль и средства теленаблюдения), так и потому, что они не являются специалистами по методам машинного обучения в такой степени, чтобы корректировать обучение модели. Второй момент, который необходимо учитывать, – это склонность методов машинного обучения к чрезмерной подгонке, т. е. потере способности к обобщению. Такая ситуация, хорошо знакомая практикам в области машинного обучения, обычно выявляется при наблюдении зависимости между ошибкой обучения и тестовой ошибкой: исправленная ошибка на обучающей выборке приводит к усилению ошибки на тестовой выборке; это говорит о чрезмерной подгонке, процесс обучения нужно остановить. Последний метод является одним из самых широко известных и эффективных методов предотвращения чрезмерной подгонки; он носит название «ранней остановки» и, очевидно, не применим к системам, которые одновременно продаются «готовыми» (т. е. процесс обучения был остановлен до наступления чрезмерной подгонки) и способны обучаться вне процесса производства.

В нашем примере смарт-часы могут потерять способность к обобщению после того, как пациент пользовался ими некоторое время, как по причине некорректного использования, так и потому, что в течение этого времени наблюдения оказались несбалансированными (например, пациент болел и его сердечный ритм или анализы крови длительное время были не в норме). С правовой точки зрения это обстоятельство будет значимым не только для разработчиков согласно новому режиму ответственности ИИ, но также для нового регламента безопасности, вводимого Законом об ИИ и проектом так называемого закона о киберустойчивости. В-третьих, эти проблемы усугубляются в случае использования методов непрерывного обучения в течение всей жизни (Parisi, 2019), так как при этом система непрерывно получает новые образцы и изменяет свое поведение. Фактически такие методы

машинного обучения представляют проблему, так как новые образцы часто являются несбалансированными (например, некоторые категории представлены шире, чем другие, выше вероятность встретить их в реальном мире), что может существенно повлиять на качество обучения и будущее поведение ИИ. Так, в нашем примере со смарт-часами конкретные характеристики пациента могут привести к искажению определенных физиологических параметров и некорректному результату.

Наконец, проблема вообще не имеет решения в случае пошагового обучения на генеральной выборке (Mi, 2020), когда машина получает новые образцы, которые могут, в принципе, принадлежать новым категориям, не рассматривавшимся ранее: в этом случае алгоритм должен быть способен перестроить свое внутреннее функционирование (например, в случае глубоких нейросетей адаптировать архитектуру, изменить топологию, число нейронов, заново откалибровать все параметры), что явно противоречит любой реалистической возможности предсказать будущее поведение системы. В нашем примере пациент может иметь уникальные характеристики, не совпадающие с физиологическими показателями, заложенными в систему при обучении. Это может быть опасно для пациента, так как неверные предположения системы могут привести к назначению неправильной дозы лекарства, при этом в отсутствие врача ошибка не будет исправлена.

Предложенное дополнение к Закону об ИИ лишь поверхностно касается вопроса о непрерывном обучении в ст. 15: «<...> Высокорисковые системы ИИ, продолжающие обучаться после выпуска на рынок или запуска в работу, должны разрабатываться таким образом, чтобы гарантировать применение адекватных мер сдерживания против потенциально предвзятых результатов, получаемых из-за использования других результатов в качестве исходных данных для будущих операций (“петля обратной связи”)...» В Преамбуле 78 уточняется, что в целях обеспечения учета провайдерами высокорисковых систем ИИ опыта использования высокорисковых систем ИИ при усовершенствовании их систем и в процессе разработки и усовершенствования процессов, а также своевременного принятия всех возможных мер для их коррекции все провайдеры должны применять систему послепродажного мониторинга. Такая система является ключевым элементом, гарантирующим возможность принятия эффективных и своевременных мер против потенциальных рисков, возникающих в результате продолжающегося «обучения» после выпуска на рынок или запуска в эксплуатацию. В данном контексте провайдеры также обязаны иметь систему, позволяющую сообщать соответствующим органам власти о любых серьезных инцидентах и о нарушениях национального и общеевропейского законодательства о защите базовых прав, происшедших в результате использования принадлежащих им систем ИИ.

Данное положение сформулировано крайне расплывчато и не проясняет, какие именно возможные сдерживающие меры или коррекционные действия можно считать адекватными. Практическое применение данного параграфа будет затруднено из-за его нечеткости и возможности произвольного толкования судебными органами. Положение о «системе послепродажного мониторинга» – это полезная мера, однако она вряд ли может быть эффективной в приложении к персонализированной медицине, поскольку производители не могут постоянно следить за каждым пациентом. Непрерывное обучение во многих отношениях представляет собой большую правовую проблему (Marchant & Lindor, 2012).

Например, она ставит под сомнение традиционную парадигму ответственности: возможно ли адаптировать режим строгой ответственности к ситуации, когда ни разработчик, ни производитель не могут предсказать поведение ИИ? Кроме того, безопасен ли с технической точки зрения для пациентов продукт, действия которого нельзя полностью объяснить, даже если его обучение осуществляется производителем? Исследователями была выдвинута так называемая теория пробела ответственности (Matthias, 2004), однако другие ученые ее отвергают (Tigard, 2020).

В таких случаях очень сложно предусмотреть профессиональную ответственность со стороны врача. Возникает также множество вопросов относительно охраны неприкосновенности частной жизни. Например, поскольку сотрудники системы здравоохранения не контролируют способ, которым указанные системы обрабатывают данные о здоровье пациентов, то они не могут полностью соблюсти свои обязанности в области прозрачности деятельности. В следующем разделе мы рассмотрим проблемы неприкосновенности частной жизни.

4. Вопросы охраны частной жизни в телемедицине

Один из самых актуальных вопросов в сфере телемедицины и искусственного интеллекта – это, несомненно, вопрос охраны персональных данных, и в частности Европейский регламент № 679/2016 (Общий регламент ЕС по защите персональных данных, GDPR). Согласно этому регламенту, данные о здоровье, наряду с некоторыми другими, относятся к «особым категориям данных» (ст. 9) и требуют повышенной правовой защиты.

В телемедицине, как и в традиционной медицине, осуществляется обработка особых категорий персональных данных, а именно данных о здоровье. Данные пациентов, которыми пользуются модели ИИ в здравоохранении, редко могут быть полностью анонимными; чаще всего считается, что они псевдонимизированы, так как медицинское учреждение может сопоставить их с именами и другими личными данными пациентов.

Даже если телемедицинские устройства не основаны на ИИ, личности пациентов большую часть времени известны медицинским работникам, так как цель системы здравоохранения – предоставлять медицинскую помощь конкретному лицу. При этом применяются Общий регламент ЕС по защите персональных данных и другие нормы в области охраны неприкосновенности частной жизни (такие как законы отдельных стран, внутренние отраслевые положения и т. д.). Из-за способа, которым осуществляется телемедицинская деятельность, неизбежно будет возникать ряд вопросов в сфере частной жизни.

Самый очевидный из них – это вопрос безопасности, поскольку взаимодействие на расстоянии предполагает установление связи между участниками (между врачом и пациентом или между несколькими медицинскими работниками). Должны выполняться меры безопасности, предусмотренные ст. 32 Общего регламента ЕС по защите персональных данных: необходимо гарантировать, что используется безопасное соединение, что личности пациента и врача подтверждены, что все задействованные лица имеют адекватную подготовку, что данные корректно хранятся, а когда перестают быть нужными – уничтожаются. Риск утечки данных особенно высок в случае работы с пожилыми пациентами, которые обычно не знакомы с новыми технологиями. Устройства интернета вещей могут теряться, пароли взламываются недобросовестными пользователями, данные могут быть удалены по ошибке. Сам факт нахождения устройства в руках пациента означает, что специалисты в области здравоохранения и информационных технологий в этот момент не контролируют систему.

Поэтому до введения таких устройств пациент должен получить адекватную подготовку. Однако недавние атаки на информационные системы больниц показали, что применяемые ими организационные меры не всегда отвечают поставленным задачам, главным образом из-за недостаточной подготовки и низкого уровня знаний о кибербезопасности у персонала (Gioulekas, 2022).

Предоставляя услуги телемедицины, медицинские учреждения должны убедиться, что они могут выполнить все требования ст. 32 Общего регламента ЕС по защите персональных данных, включая подготовку своего персонала в области основных мер кибербезопасности. Если медицинский работник не способен обучиться мерам безопасности, то он, вероятно, не сможет и контролировать взаимодействие пациентов с системой. Не будучи техническими специалистами, они, вероятно, не смогут также определить сбои в системе, такие как некорректное обучение нейросети. В этом контексте необходимо, чтобы устройство регулярно подвергалось проверке, обновлению и калибровке со стороны специалистов по ИИ. Дополнительные гарантии в отношении особых категорий данных предусмотрены Законом об ИИ в последнем разделе ст. 10: они должны обрабатываться в той мере, которая необходима для целей предотвращения необъективности, обнаружения и коррекции в отношении высокорисковых систем ИИ, однако при этом необходимы соответствующие гарантии (такие как технические ограничения на повторное использование данных, а также применение новейших технических средств, включая псевдонимизацию или шифрование).

При использовании системы ИИ для предоставления услуг телемедицины необходимо на уровне разработки по умолчанию внедрить в эту систему принципы охраны частной жизни, принимая во внимание также принципы минимизации данных и ограничения по их хранению. С этой целью в Преамбуле 44 предусмотрена дополнительная задача обработки персональных медицинских данных, а именно «мониторинг, обнаружение и коррекция необъективности» для создания справедливых и надежных систем ИИ.

Выполнение вышеупомянутых требований может быть затруднено в случае непрерывного обучения: как можно гарантировать точность, обновляемость и минимизацию данных, если нельзя предсказать поведение системы? Еще одна общая проблема телемедицины касается передачи медицинских данных за рубеж. В момент консультации пациент и доктор могут находиться в разных странах, а значит, в разных юрисдикциях.

Эта проблема уникальна для телемедицины, поскольку область медицинских консультаций строго регулируется в каждой стране мира, где существуют различные нормы в отношении согласия, прозрачности, стандартов качества, ответственности, страхования, защиты данных, безопасности, установления личности, договорных отношений, оплаты, профессиональной этики и т. д. Каждый из этих элементов может стать предметом судебного разбирательства или официального расследования, создавая правовые коллизии. Некоторые из этих аспектов регулируются договорами, но большинство регулируются напрямую международным правом и не могут быть изменены по договору. Если возникает спорная ситуация, то пациенту, который уже находится в невыгодном положении, будет крайне сложно добиться компенсации и правовой помощи. Даже если договорные отношения возможны, может быть непросто достичь соглашения относительно обязанностей и ответственности в условиях непредсказуемости системы.

Таким образом, уровень риска повышен в сравнении с очными консультациями, тогда как крайняя неопределенность в поведении системы осложняет регулирование отношений между пациентом и доктором. Кроме того, устройство, применяемое при оказании услуги, может пользоваться облачными решениями на серверах, находящихся за пределами ЕС.

Из-за характера используемых данных риски для пациента оказываются выше, чем в других областях. Хотя и после обычной очной консультации врач может поместить данные пациента в зарубежные облачные хранилища, разница с непрерывно обучающимися устройствами состоит в том, что информация может изменяться и обновляться в режиме реального времени, тем самым предоставляя актуальные и истинные данные потенциальным хакерам, властям зарубежных стран, производителям системы. Если устройство не собирает и не использует информацию в режиме реального времени, то пациентам проще контролировать свои данные, удалять их, отбирать данные для хранения и загрузки в модель, получать к ним доступ, как требует новый проект так называемого Закона о данных. Перед использованием таких систем необходима их тщательная оценка, возможно, с помощью инструмента «Оценка воздействия на защиту данных» (Data Protection Impact Assessment, DPIA). Кроме того, возможно, понадобится соответствующее соглашение в области защиты данных между медицинским учреждением и производителями телемедицинских устройств.

5. Статья 22 Общего регламента ЕС по защите персональных данных и контроль со стороны человека

Использование устройств на основе ИИ в телемедицине часто подпадает под определение автоматизированного принятия решений (АПР) и профилирования (ст. 22), например, в случае автоматического сканирования медицинского изображения при постановке диагноза. Наряду с принципом прозрачности, который гарантирует субъектам данных право на информирование о том, как будут использоваться их данные, и о последствиях их обработки, Общий регламент ЕС по защите персональных данных также гарантирует дополнительное право в отношении АПР и профилирования: право на объяснение. Это означает, что «контролирующая сторона обязана простым способом объяснить субъекту данных основания и критерии принятого решения, не пытаясь прибегать к сложным объяснениям применяемых алгоритмов или полному раскрытию алгоритма. При этом предоставляемая информация должна быть понятна субъекту данных»[6].

В этом контексте модели, работающие по принципу «черного ящика», в особенности основанные на непрерывном обучении, не отвечают этому требованию, поскольку пациенту невозможно объяснить, почему модель пришла к определенному результату. В руководстве отмечается: «Сложность не является причиной непредоставления информации субъекту данных. Преамбула 58 предусматривает, что принцип прозрачности непосредственно относится к ситуациям, когда быстрое нарастание количества действующих лиц и технологической сложности деятельности

6 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053/en

затрудняет понимание субъектом данных факта сбора относящихся к нему данных и того, кем и с какой целью они собираются, как, например, в случае онлайн-рекламы»[7]. Это особенно важно в контексте телемедицины, где речь идет о медицинских данных, а пациент не находится под непосредственным наблюдением врача. Последствия ошибки могут доходить до летальных исходов, и в этом одна из причин, по которым Еврокомиссия классифицировала медицинские устройства как «высокорисковые системы».

Сторона, контролирующая данные, например больница или производитель телемедицинского устройства, обязана предоставить информацию об обработке данных и о возможном влиянии АПР и профилирования на субъектов данных. Статья 77 Конвенции 108+ гласит: «Субъекты данных вправе знать основания для обработки данных, включая следствия из этих оснований, приводящие к любым полученным выводам, в частности, в случаях использования алгоритмов автоматизированного принятия решений и профилирования. Например, при выставлении кредитного рейтинга субъект имеет право знать логику обработки данных, приведшую к положительному или отрицательному решению, а не просто информацию о вынесенном решении. Понимание этих элементов способствует эффективному осуществлению иных существенных гарантий, таких как право на возражение и право на обращение к уполномоченным органам»[8]. Кроме того, субъекты данных имеют право выражать свое мнение об автоматизированном принятии решений и профилировании, право на принятие касающихся их решений человеком и право на оспаривание принятого решения. В случае телемедицины на основе ИИ может быть крайне сложно осуществлять управление процессом оказания медицинской помощи на расстоянии таким образом, чтобы врач мог контролировать каждое решение, принятое системой, и в то же время гарантировать, что решения принимает только врач, поскольку это сводит на нет все преимущества использования автоматизации. Даже если организовать постоянное присутствие врачей, в условиях непрерывного обучения они не смогут объяснить пациенту действия системы. Возможно, это достижимо в некоторых случаях, но в будущем, когда такие устройства получат широкое распространение и будет достигнута высокая степень интеграции телемедицины в систему здравоохранения на низовом уровне, тщательное наблюдение за указанными аспектами станет чрезвычайно важным. Еще одна большая проблема с системами непрерывного обучения состоит в сложности обеспечения права на оспаривание решения системы, т. е. «недостаток очевидных средств для оспаривания результатов, которые представляются неожиданными, вредными, несправедливыми или дискриминирующими» (Edwards & Veale, 2017). Оспорить решение системы не может не только пациент, но и врач, работающий удаленно, так как для этого нужно собрать все элементы, использованные системой при вынесении данного решения (например, изменения дозировки лекарства). Таким образом, предложение о «встроенной оспариваемости» (Almada, 2019) изначально неприменимо к таким моделям. В рамках этого сценария можно утверждать, что в интересах прозрачности и справедливости стандартом для телемедицины должны стать интерпретируемые модели ИИ, тогда как «черные ящики» должны использоваться

---

7 *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053

8 *Там же.* Art. 29.

только в тех случаях, когда медицинский работник может тщательно контролировать результаты, выдаваемые системой, и выносить общую клиническую оценку на основе дополнительных по отношению к системе ИИ элементов. Кроме того, системы непрерывного обучения должны быть ограничены лишь теми решениями, которые не могут нанести вред пациенту в случае ошибок, и должны постоянно проверяться врачебным персоналом.

6. Информированное согласие

Когда правовой основой для обработки медицинских данных пациента является его согласие, как это часто бывает в случае телемедицинских устройств, то, согласно Общему регламенту ЕС по защите персональных данных, такое согласие должно быть явным, информированным, свободно выраженным, конкретным и недвусмысленным. Помимо обычных элементов, которые сообщаются субъекту данных согласно действующему законодательству, должна быть предоставлена также дополнительная информация о порядке проведения виртуальной консультации. Сюда включается информация о правах в рамках законов о защите данных, о возможных ошибках системы, о протоколах связи во время телеконсультаций, о правилах назначения лекарств и о координации работы с другими медицинскими работниками (Membrado, 2021). Дополнительные требования об обеспечении прозрачности содержатся в Законе об ИИ: в ст. 13 перечислены данные, которые должны быть предоставлены пользователям при инструктировании по поводу работы системы ИИ, а именно: высокорисковые системы ИИ должны сопровождаться инструкцией по использованию в соответствующем цифровом или ином формате, включая сжатую, полную, корректную и четкую информацию, релевантную, доступную и понятную пользователям. Статьи 11 и 18 содержат требование о подробной технической документации, которую следует обновлять перед выпуском системы. В руководствах по автоматизированному принятию решений отмечается, что если сторона, контролирующая данные, использует согласия как основу для профилирования, то она должна продемонстрировать, что субъект данных понимает, на что именно он дает свое согласие, и помнить, что согласие не всегда служит достаточным основанием для обработки данных. Во всех случаях субъекты данных должны иметь достаточный объем релевантной информации о предполагаемом использовании своих данных и последствиях их обработки, чтобы выраженное согласие представляло собой информированный выбор. Можно утверждать, что при использовании непрерывного обучения это требование изначально невыполнимо, так как даже врач или разработчик модели не может предсказать последствия использования непредсказуемой модели. Информация, полученная пациентом, должна быть сжатой, прозрачной, понятной, доступной, изложенной простым языком, учитывающей такие особенности, как возраст, умственные способности и уровень образования субъекта данных. В любом случае автоматизированное принятие решений и профилирование с использованием особых категорий данных, таких как медицинские данные, возможно лишь при наличии явного согласия субъекта данных или если это предусмотрено законом в существенных интересах общества, при условии наличия адекватных защитных механизмов. Интересы общества не являются достаточным законным основанием, их важность должна быть подтверждена. Например, можно утверждать, что борьба с инфекцией Covid-19 является «существенным интересом общества».

Информированное согласие как с правовой, так и с этической точек зрения становится центральным элементом систем ИИ, применяемых в телемедицине.

7. Уязвимые группы

Актуальная проблема телемедицины с использованием систем искусственного интеллекта вызывает еще большую озабоченность, когда касается особенно уязвимых субъектов, таких как онкологические пациенты, пациенты с когнитивными нарушениями, например, пожилые люди, страдающие старческой деменцией или болезнью Альцгеймера, дети, нейроотличные пациенты (Shaw et al., 2022), люди, не владеющие языком, на котором говорит доктор. В первую очередь необходимо дать им возможность выразить свое информированное, свободное, однозначное и конкретное согласие (ст. 7 Общего регламента ЕС по защите персональных данных). Отношения между врачом и пациентом сами по себе не являются сбалансированными, так как стороны в них находятся на разных уровнях, а позиция пациента уязвима; поэтому может быть непросто получить согласие, отвечающее всем требованиям закона, от такого уязвимого человека, как, например, онкологический пациент, уже подавленный своей болезнью.

Если прибавить сюда право пациента на объяснение, то становится ясно, что возникает сразу несколько сложных проблем: в условиях телемедицины доктор находится вдали от пациента, человеческий контакт недостаточен. В таких условиях объяснения могут оказаться нечеткими или непонятными, поскольку пациент не может распознать знаки невербальной коммуникации.

При использовании систем искусственного интеллекта, работа которых часто непонятна и специалистам, даже когда эта система обладает свойствами объяснимости и интерпретируемости, риски непонимания еще более возрастают и становятся труднопреодолимыми, если только консультации не проводятся также в очном формате. Если действия системы непредсказуемы, то уязвимому пациенту еще сложнее объяснить последствия применения устройства.

Нельзя забывать и о явлении цифрового неравенства, т. е. о том, что не все пациенты обладают одинаковым уровнем цифровой грамотности. Это обстоятельство приобретает особую значимость, когда услуги телемедицины оказываются в государственном секторе, так как именно там высока вероятность дискриминации между теми, кто способен воспользоваться этими услугами, и теми, кто по разным причинам не способен этого сделать. Этот аспект подчеркивался в заявлении Еврокомиссии, которое было основано, в частности, на докладе ОЭСР «Краткий обзор вопросов здравоохранения: Европа – 2018», где говорилось об этой проблеме.

Комиссия отметила наличие прямой зависимости между уровнем образования и числом запросов на поиск медицинской информации в Сети; фактически вполне вероятны подобные несоответствия в использовании цифровых решений для улучшения здоровья и предотвращения заболеваемости, а значит, риск того, что цифровые инструменты: приложения, носимые устройства, онлайн-форумы – не принесут пользы тем, кто в них более всего нуждается, что потенциально усилит неравенство в области охраны здоровья (Oliveira, 2020). Этот разрыв может даже увеличиться из-за систем непрерывного обучения, так как лица, лучше владеющие технологиями телемедицины, будут получать более точные результаты. Этот риск должен учитываться специалистами в области здравоохранения при оказании телемедицинских услуг.

8. Баланс между охраной неприкосновенности частной жизни и защитой от вреда при дистанционной работе

Как обсуждалось выше, одна из важнейших проблем с системами непрерывного обучения в телемедицине состоит в том, что модель «развивается», когда пациент находится далеко от доктора (от специалистов технической поддержки), но при этом системы обычно разрабатываются так, чтобы быть как можно менее инвазивными. Это приводит к необходимости балансировать между постоянным наблюдением за пациентами с целью обеспечения их безопасности и охраной их частной жизни, чтобы применение технологий не доставляло им неудобств. Таким образом, релевантными оказываются четыре аспекта: технические меры, организационные меры, психологические факторы и требования закона. С технической точки зрения изучались несколько методов решения проблем неприкосновенности частной жизни, которые обсуждались выше, например, проблема идентификации личности с использованием блокчейна, шифрования, федеративного обучения с помощью концепции периферийных вычислений (Ahmad, 2021; Jain et al., 2022; Wang, 2021, Ma et al., 2020; Wang, 2022).

Однако некоторые проблемы невозможно решить лишь с помощью технологий: организационные меры играют решающую роль в достижении баланса между охраной частной жизни и преимуществами технологии наблюдения как меры противодействия неожиданным сбоям в системе.

Фактически в качестве первоочередной меры для снижения ущерба от сбоя системы, можно запланировать необходимые поддерживающие вмешательства со стороны технических специалистов и медиков, которые могут тестировать систему, оценивать ее работу и состояние здоровья пациента. Такие действия можно проводить с минимальным уровнем беспокойства для пациентов (например, совмещая проверки с регулярными очными приемами в медицинском учреждении). Однако вторая мера не менее значима: это обучение врачей и пациентов корректному использованию технологий телемедицины, что чрезвычайно важно как для сохранения неприкосновенности частной жизни, так и для снижения риска сбоя системы и ее некорректного использования. При условии качественной подготовки врачи смогут, например, распознать такие особенности пациентов, которые могут привести самообучающуюся систему к генерации ошибочных выводов.

С психологической точки зрения уязвимые пациенты могут нуждаться в дополнительной поддержке в областях: понимания работы системы, чтобы корректно ее использовать и свободно выражать свое информированное согласие; принятия системы как части своей жизни без чувства нарушения повседневной деятельности; обучения выражению своего беспокойства и неудобства (включая физическую боль) на расстоянии (Yakar, 2021).

Обученный терапевт, работая совместно с техническими специалистами и профильными медиками, может помочь пациентам справляться с этими проблемами. С другой стороны, врачи должны удостовериться, что пациенты понимают их указания, и регулярно проверять, что даваемое пациентами согласие действительно является информированным. Нормы о неприкосновенности частной жизни не препятствуют тому, чтобы задействовать вышеописанные меры, так как Общий регламент ЕС по защите персональных данных предусматривает соответствующие способы защиты фундаментальных прав пациентов. В качестве дополнительной организационной меры больницы должны иметь специалиста по вопросам охраны частной жизни, который следил бы за использованием телемедицинских устройств и консультировал всех заинтересованных лиц.

9. Меры дополнительной защиты в форме аудита искусственного интеллекта

В последние годы все большую популярность приобретает научная область алгоритмического аудита в рамках более широкой проблемы аудита ИИ, особенно в отношении машинного обучения. Аудит ИИ предполагает встраивание вопросов этики, прав человека и законности во все стадии жизненного цикла ИИ от разработки до послепродажного функционирования (LaBrie & Steinke, 2019; Mökander & Floridi, 2022; Mantelero & Esposito, 2021; Koshiyama et al., 2021; Mökander, 2022; Floridi, 2022) с одновременным контролем его технических характеристик (а именно безопасности, эффективности, корректности методов обработки данных). С этой целью был разработан ряд практических инструментов, таких как дискуссии по вопросам этики (например, дискуссии по открытому ИИ, по этике данных, по этике ИИ (Kalra, 2020)). Такая форма оценки и непрерывного мониторинга важна для выявления предубеждений, технических и статистических ошибок, дефектов в системе безопасности, неблагоприятных эффектов на послепродажном этапе. Фактически благодаря пристальному вниманию к процессу в целом и к механизму обеспечения соответствия, применяемому с самых первых этапов развития ИИ (т. е. еще до этапа сбора данных) оказалось возможным предотвратить целый ряд ошибок, которые могли привести к нарушению принципа неприкосновенности частной жизни, сбоям в системе, дефе там в системе безопасности, дискриминации. В связи с этим рекомендуется применять процедуры аудита ИИ каждый раз, когда в клинической практике задействованы модели непрерывного обучения.

Заключение

В этой краткой работе мы постарались показать, как телемедицина с помощью интеллектуальных систем непрерывного обучения становится полезным инструментом для усовершенствования медицинского обслуживания пациента, однако ее распространение может также поставить новые вопросы перед юристами и медиками. Новые правовые проблемы, такие как регулирование систем, адаптирующихся к потребностям пациента, или защита уязвимых субъектов, их способность понять работу ИИ для свободного выражения своего согласия, должны в ближайшее время быть рассмотрены и решены в рамках правовой доктрины. Медицинские учреждения, планирующие использовать системы ИИ для оказания телемедицинских услуг, должны обучить персонал и пациентов безопасному обращению с системой, чтобы избежать утечки данных и некорректного использования устройств. Эффективно достичь этой цели можно с помощью сплоченного коллектива технических специалистов, профильных врачей и обученных врачей общей практики. Хотя в Евросоюзе предпринимались попытки давать правовые ответы на вопросы, связанные с развитием технологий ИИ, остается еще много нерешенных проблем. Поэтому стоит надеяться, что данная область будет тщательно изучена, прежде чем телемедицина с использованием ИИ получит широкое распространение и войдет в повседневную практику на территории Евросоюза.

Список литературы

Ahmad, R. W. (2021). The role of blockchain technology in telehealth and telemedicine. *International Journal of Medical Informatics*, *148*, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

Almada, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. In *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (pp. 2–11). https://doi.org/10.2139/ssrn.3264189

Botrugno, C. (2014). Un diritto per la telemedicina: analisi di un complesso normativo in formazione. *Politica del Diritto*, *4*(45), 639–668. https://doi.org/10.1437/78949

Burrai, F., Gambella, M., & Scarpa, A. (2021). L'erogazione diprestazioni sanitarie in telemedicina. *Giornale di Clinica Nefrologica e Dialisi*, *33*, 3–6.

Campagna, M. (2020). Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19. *Corti Supreme e Salute*, *3*, 11–25.

Castagno, S., & Khalifa, M. (2020). Perceptions of artificial intelligence among healthcare staff: a qualitative survey study. *Frontiers in artificial intelligence*, *2*(5), 84–92. https://doi.org/10.3389/frai.2020.578983

Davis, E. (2016). AI Amusements: The Tragic Tale of Tay the Chatbot. *AI Matters*, *2*(4), 20–24. https://doi.org/10.1145/3008665.3008674

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18–26.

Floridi, L. (2022). capAI-A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4064091

Gallese, Ch. (2022). Suggestions for a revision of the European smart robot liability regime. In *Proceedings of the 4th European Conference on the Impact of Artificial Intelligence and Robotics (ECIAIR 2022)*. https://doi.org/10.34190/eciair.4.1.851

Gioulekas, F. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327–333. https://doi.org/10.3390/healthcare10020327

Giunti, G. (2014). The Use of a Gamified Platform To Empower And Increase Patient Engagement in Diabetes Mellitus Adolescents. In *American Medical Informatics Association Annual Symposium*.

Jain, N., Gupta V., & Dass, P. (2022). Blockchain: A novel paradigm for secured data transmission in telemedicine. In *Wearable Telemedicine Technology for the Healthcare Industry* (pp. 33–52).

Kalra, A. (2020). *Artificial Intelligence Ethics Canvas: A Tool for Ethical and Socially Responsible AI*.

Koshiyama, A. S., Kazim, E., Treleaven, P. C., Rai, P., Szpruch, L., Pavey, G., Ahamat, G., Leutner, F., Goebel, R., Knight, A., Adams, J., Hitrova, C., Barnett, J., Nachev, P., Barber, D., Chamorro-Premuzic, T., Klemmer, K., Gregorovic, M., Khan, S. A., & Lomas, E. (2021). Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms. *Software Engineering eJournal*. https://doi.org/10.2139/ssrn.3778998

LaBrie, R., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. In *Twenty-fifth Americas Conference on Information Systems*.

Lakkaraju, H. (2019). Faithful and customizable explanations of black box models. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 131–138). https://doi.org/10.1145/3306618.3314229

Ma, M., Shuqin, F., & Feng, D. (2020). Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. *Journal of Information Security and Applications*, *55*, 102652. https://doi.org/10.1016/j.jisa.2020.102652

Mantelero, A., & Esposito, S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Marchant, G., & Lindor, R. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*, 1321–1340.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and information technology*, *6*, 175–183. https://doi.org/10.1007/s10676-004-3422-1

Membrado, C. G. (2021). Telemedicina, ética y derecho en tiempos de COVID-19. Una mirada hacia el futuro. *Revista Clinica Espanola*, *221*, 408–410. https://doi.org/10.1016/j.rce.2021.03.002

Mi, F. (2020). Generalized Class Incremental Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 240–241).

Mökander, J. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*, 241–268. https://doi.org/10.1007/s11023-021-09577-4

Mökander, J., & Floridi, L. (2022). Operationalising AI governance through ethics-based auditing: an industry case study. *AI and Ethics*, *6*, 1–18. https://doi.org/10.1007/s43681-022-00171-7

Oliveira, T. (2020). Bringing health care to the patient: An overview of the use of telemedicine in OECD countries. *OECD, Directorate for Employment, Labour and Social Affairs, Health Committee*.

Pacis, D., Mitch, M., Edwin, D. C., Subido, Jr., & Bugtai, N. (2018). Trends in telemedicine utilizing artificial intelligence. In *AIP conference proceedings*. AIP Publishing LLC.

Parisi, G. (2019). Continual lifelong learning with neural networks: A review, *Neural Networks*, *113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005

Schatten, M., & Protrka, R. (2021). Conceptual Architecture of a Cognitive Agent for Telemedicine based on Gamification. In *Central European Conference on Information and Intelligent Systems* (pp. 3–10).

Scheetz, J. (2021). A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Scientific reports*, *11.1*, 1–10.

Shaw, S., Davis, L-J., & Doherty, M. (2022). *Considering autistic patients in the era of telemedicine: the need for an adaptable, equitable, and compassionate approach, BJGP open 6.1*.

Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics? *Archives of disease in childhood*, *91.12*, 956–959. https://doi.org/10.1136/adc.2006.099622

Tigard, D. (2020). There is no techno-responsibility gap. *Philosophy & Technology*, 1–19.

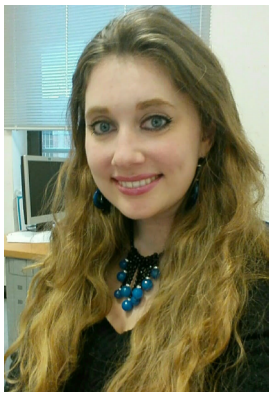
Wang, R. (2022). Privacy-Preserving Federated Learning for Internet of Medical Things under Edge Computing. *IEEE Journal of Biomedical and Health Informatics*.

Wang, W. (2021). A privacy protection scheme for telemedicine diagnosis based on double blockchain. *Journal of Information Security and Applications*, *61*, 102845. https://doi.org/10.1016/j.jisa.2021.102845

Yakar, D. (2021). Do People Favor Artificial Intelligence Over Physicians? A Survey Among the General Population and Their View on Artificial Intelligence in Medicine. *Value in Health*, *3*, 12–23. https://doi.org/10.1016/j.jval.2021.09.004

Ye, J. (2020). The role of health technology and informatics in a global public health emergency: practices and implications from the COVID-19 pandemic. *JMIR medical informatics*, *8.7*, e19866. https://doi.org/10.2196/19866

Сведения об авторе



Галлезе-Нобиле Кьяра – доктор наук, научный сотрудник (постдок) по управлению исследовательскими данными, Эйндховенский технологический университет (Эйндховен, Королевство Нидерландов); научный сотрудник (постдок) департамента математики и наук о земле, Университет Триеста (Триест, Итальянская Республика)
Адрес: а/я 513 5600 МБ Эйндховен, Королевство Нидерландов
E-mail: cgallese@liuc.it
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57222726276
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/AGE-9594-2022
ORCID ID: https://orcid.org/0000-0001-8194-0261
Google Scholar ID: https://scholar.google.com/citations?user=Vmoen8UAAAAJ

Конфликт интересов

Автор является международным редактором журнала, статья прошла рецензирование на общих основаниях.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.27.91 / Гражданское право отдельных стран
Специальность ВАК: 5.1.3 / Частно-правовые (цивилистические) науки

История статьи

Дата поступления – 4 мая 2023 г.
Дата одобрения после рецензирования – 20 мая 2023 г.
Дата принятия к опубликованию – 16 июня 2023 г.
Дата онлайн-размещения – 20 июня 2023 г.

Research article
DOI: https://doi.org/10.21202/jdtl.2023.13

Legal Aspects of the Use Artificial Intelligence in Telemedicine

Chiara Gallese Nobile

Eindhoven University of Technology
Eindhoven, Netherlands;
University of Trieste
Trieste, Italy

Keywords

Artificial intelligence,
data protection,
digital inequality,
digital technologies,
law,
legislation,
personal data,
private life,
regulation,
telemedicine

Abstract

Objective: the rapid expansion of the use of telemedicine in clinical practice and the increasing use of Artificial Intelligence has raised many privacy issues and concerns among legal scholars. Due to the sensitive nature of the data involved particular attention should be paid to the legal aspects of those systems. This article aimed to explore the legal implication of the use of Artificial Intelligence in the field of telemedicine, especially when continuous learning and automated decision-making systems are involved; in fact, providing personalized medicine through continuous learning systems may represent an additional risk. Particular attention is paid to vulnerable groups, such as children, the elderly, and severely ill patients, due to both the digital divide and the difficulty of expressing free consent.

Methods: comparative and formal legal methods allowed to analyze current regulation of the Artificial Intelligence and set up its correlations with the regulation on telemedicine, GDPR and others.

Results: legal implications of the use of Artificial Intelligence in telemedicine, especially when continuous learning and automated decision-making systems are involved were explored; author concluded that providing personalized medicine through continuous learning systems may represent an additional risk and offered the ways to minimize it. Author also focused on the issues of informed consent of vulnerable groups (children, elderly, severely ill patients).

Scientific novelty: existing risks and issues that are arising from the use of Artificial Intelligence in telemedicine with particular attention to continuous learning systems are explored.

Practical significance: results achieved in this paper can be used for lawmaking process in the sphere of use of Artificial Intelligence in telemedicine and as base for future research in this area as well as contribute to limited literature on the topic.

For citation

Gallese Nobile, C. (2023). Legal Aspects of the Use Artificial Intelligence in Telemedicine. *Journal of Digital Technologies and Law, 1*(2), 314–336. https://doi.org/10.21202/jdtl.2023.13

References

Ahmad, R. W. (2021). The role of blockchain technology in telehealth and telemedicine. *International Journal of Medical Informatics*, *148*, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

Almada, M. (2019). Human intervention in automated decision-making: Toward the construction of contestable systems. In *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law* (pp. 2–11). https://doi.org/10.2139/ssrn.3264189

Botrugno, C. (2014). Un diritto per la telemedicina: analisi di un complesso normativo in formazione. *Politica del Diritto*, *4*(45), 639–668. https://doi.org/10.1437/78949

Burrai, F., Gambella, M., & Scarpa, A. (2021). L'erogazione diprestazioni sanitarie in telemedicina. *Giornale di Clinica Nefrologica e Dialisi*, *33*, 3–6.

Campagna, M. (2020). Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19. *Corti Supreme e Salute*, *3*, 11–25.

Castagno, S., & Khalifa, M. (2020). Perceptions of artificial intelligence among healthcare staff: a qualitative survey study. *Frontiers in artificial intelligence*, *2*(5), 84–92. https://doi.org/10.3389/frai.2020.578983

Davis, E. (2016). AI Amusements: The Tragic Tale of Tay the Chatbot. *AI Matters*, *2*(4), 20–24. https://doi.org/10.1145/3008665.3008674

Edwards, L., & Veale, M. (2017). Slave to the algorithm: Why a right to an explanation is probably not the remedy you are looking for. *Duke L. & Tech. Rev.*, *16*, 18–26.

Floridi, L. (2022). capAI-A Procedure for Conducting Conformity Assessment of AI Systems in Line with the EU Artificial Intelligence Act. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4064091

Gallese, Ch. (2022). Suggestions for a revision of the European smart robot liability regime. In *Proceedings of the 4th European Conference on the Impact of Artificial Intelligence and Robotics (ECIAIR 2022)*. https://doi.org/10.34190/eciair.4.1.851

Gioulekas, F. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare*, *10*, 327–333. https://doi.org/10.3390/healthcare10020327

Giunti, G. (2014). The Use of a Gamified Platform To Empower And Increase Patient Engagement in Diabetes Mellitus Adolescents. In *American Medical Informatics Association Annual Symposium*.

Jain, N., Gupta V., & Dass, P. (2022). Blockchain: A novel paradigm for secured data transmission in telemedicine. In *Wearable Telemedicine Technology for the Healthcare Industry* (pp. 33–52).

Kalra, A. (2020). *Artificial Intelligence Ethics Canvas: A Tool for Ethical and Socially Responsible AI*.

Koshiyama, A. S., Kazim, E., Treleaven, P. C., Rai, P., Szpruch, L., Pavey, G., Ahamat, G., Leutner, F., Goebel, R., Knight, A., Adams, J., Hitrova, C., Barnett, J., Nachev, P., Barber, D., Chamorro-Premuzic, T., Klemmer, K., Gregorovic, M., Khan, S. A., & Lomas, E. (2021). Towards Algorithm Auditing: A Survey on Managing Legal, Ethical and Technological Risks of AI, ML and Associated Algorithms. *Software Engineering eJournal*. https://doi.org/10.2139/ssrn.3778998

LaBrie, R., & Steinke, G. (2019). Towards a framework for ethical audits of AI algorithms. In *Twenty-fifth Americas Conference on Information Systems*.

Lakkaraju, H. (2019). Faithful and customizable explanations of black box models. In *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society* (pp. 131–138). https://doi.org/10.1145/3306618.3314229

Ma, M., Shuqin, F., & Feng, D. (2020). Multi-user certificateless public key encryption with conjunctive keyword search for cloud-based telemedicine. *Journal of Information Security and Applications*, *55*, 102652. https://doi.org/10.1016/j.jisa.2020.102652

Mantelero, A., & Esposito, S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems. *Computer Law & Security Review*, *41*, 105561. https://doi.org/10.1016/j.clsr.2021.105561

Marchant, G., & Lindor, R. (2012). The coming collision between autonomous vehicles and the liability system. *Santa Clara Law Review*, *52*, 1321–1340.

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and information technology*, *6*, 175–183. https://doi.org/10.1007/s10676-004-3422-1

Membrado, C. G. (2021). Telemedicina, ética y derecho en tiempos de COVID-19. Una mirada hacia el futuro. *Revista Clinica Espanola*, *221*, 408–410. https://doi.org/10.1016/j.rce.2021.03.002

Mi, F. (2020). Generalized Class Incremental Learning. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops* (pp. 240–241).

Mökander, J. (2022). Conformity assessments and post-market monitoring: a guide to the role of auditing in the proposed European AI regulation. *Minds and Machines*, *32*, 241–268. https://doi.org/10.1007/s11023-021-09577-4

Mökander, J., & Floridi, L. (2022). Operationalising AI governance through ethics-based auditing: an industry case study. *AI and Ethics*, *6*, 1–18. https://doi.org/10.1007/s43681-022-00171-7

Oliveira, T. (2020). Bringing health care to the patient: An overview of the use of telemedicine in OECD countries. *OECD, Directorate for Employment, Labour and Social Affairs, Health Committee*.

Pacis, D., Mitch, M., Edwin, D. C., Subido, Jr., & Bugtai, N. (2018). Trends in telemedicine utilizing artificial intelligence. In *AIP conference proceedings*. AIP Publishing LLC.

Parisi, G. (2019). Continual lifelong learning with neural networks: A review, *Neural Networks*, *113*, 54–71. https://doi.org/10.1016/j.neunet.2019.01.012

Rodrigues, R. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, *4*, 100005. https://doi.org/10.1016/j.jrt.2020.100005

Schatten, M., & Protrka, R. (2021). Conceptual Architecture of a Cognitive Agent for Telemedicine based on Gamification. In *Central European Conference on Information and Intelligent Systems* (pp. 3–10).

Scheetz, J. (2021). A survey of clinicians on the use of artificial intelligence in ophthalmology, dermatology, radiology and radiation oncology. *Scientific reports*, *11.1*, 1–10.

Shaw, S., Davis, L-J., & Doherty, M. (2022). *Considering autistic patients in the era of telemedicine: the need for an adaptable, equitable, and compassionate approach, BJGP open 6.1*.

Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics? *Archives of disease in childhood*, *91.12*, 956–959. https://doi.org/10.1136/adc.2006.099622

Tigard, D. (2020). There is no techno-responsibility gap. *Philosophy & Technology*, 1–19.

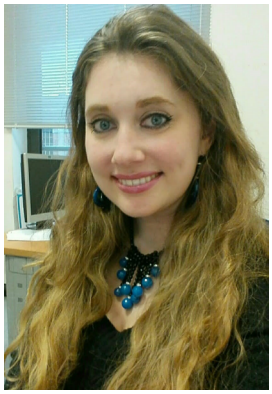
Wang, R. (2022). Privacy-Preserving Federated Learning for Internet of Medical Things under Edge Computing. *IEEE Journal of Biomedical and Health Informatics*.

Wang, W. (2021). A privacy protection scheme for telemedicine diagnosis based on double blockchain. *Journal of Information Security and Applications*, *61*, 102845. https://doi.org/10.1016/j.jisa.2021.102845

Yakar, D. (2021). Do People Favor Artificial Intelligence Over Physicians? A Survey Among the General Population and Their View on Artificial Intelligence in Medicine. *Value in Health*, *3*, 12–23. https://doi.org/10.1016/j.jval.2021.09.004

Ye, J. (2020). The role of health technology and informatics in a global public health emergency: practices and implications from the COVID-19 pandemic. *JMIR medical informatics*, *8.7*, e19866. https://doi.org/10.2196/19866

Author information



Chiara Gallese Nobile – PhD, Researcher (postdoc) of research data management, Eindhoven University of Technology (Eindhoven, Netherlands), Researcher (postdoc) of the Department of Mathematics and Geosciences, University of Trieste (Trieste, Italy).
Address: P/O 513 5600 MB Eindhoven, the Netherlands
E-mail: cgallese@liuc.it
Scopus Author ID: https://www.scopus.com/authid/detail.uri?authorId=57222726276
Web of Science Researcher ID:
https://www.webofscience.com/wos/author/record/AGE-9594-2022
ORCID ID: https://orcid.org/0000-0001-8194-0261
Google Scholar ID: https://scholar.google.com/citations?user=Vmoen8UAAAAJ

Conflict of interests

The author is an international editor of the Journal; the article has been reviewed on general terms.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – May 4, 2023
Date of approval – May 20, 2023
Date of acceptance – June 16, 2023
Date of online placement – June 20, 2023