ЮРИДИЧЕСКИЕ СЛОЖНОСТИ, СВЯЗАННЫЕ С ПРИМЕНЕНИЕМ БОЛЬШИХ МЕДИЦИНСКИХ ДАННЫХ

Имамалиева Диёра Имамали кизи
Преподаватель кафедры Международного частного права
Ташкентского государственного юридического университета
d.imamaliyeva@tsul.uz

АННОТАЦИЯ

В настоящее время глобальные системы здравоохранения претерпевают фундаментальные изменения. Мы достигли стадии серьезного перехода к способам улучшения генерации и доступа к невообразимым объемам информации. С появлением и развитием больших данных в результате информационной революции мы теперь можем управлять и трансформировать подходы, с помощью которых мы контролируем эту информацию и, в здравоохранении, как следствие, способность контролировать и лечить болезни. С другой стороны, появление больших данных в здравоохранении создает дополнительные проблемы, особенно в отношении конфиденциальности личных данных, безопасности, владения, управления и контроля. В настоящей статье раскрываются основы понимания правового статуса больших медицинских данных в подробной призме стандартов согласия, анонимизации, владения и передачи данных.

Ключевые слова: *большие данные, конфиденциальность, анонимизация данных, этические нормы, персональные данные, трансграничная передача.*

LEGAL CHALLENGES ASSOCIATED WITH THE APPLICATION OF BIG MEDICAL DATA

Imamalieva Diyora Imamali kizi
Lecturer at the Department of International Private Law
Tashkent State University of Law
d.imamaliyeva@tsul.uz

ABSTRACT

Global health systems are currently undergoing fundamental changes. We have reached a major transition in ways to improve the generation and access to unimaginable amounts of information. With the advent and development of big data as a result of the information revolution, we can now manage and transform the way

we control this information and, in healthcare, the resulting ability to monitor and treat disease. On the other hand, the emergence of big data in healthcare poses additional challenges, especially regarding personal data privacy, security, ownership, governance and control. This article provides a framework for understanding the legal status of big health data through a detailed lens on standards for consent, anonymization, ownership, and transfer of data.

Keywords: *big data, privacy, data anonymization, ethical standards, personal data, cross-border transfer.*

KATTA TIBBIY MA'LUMOTLARNI QO'LLANISH BILAN BO'LGAN HUQUQIY MUAMMOLAR

Imamalieva Diyora Imamali qizi
Toshkent davlat yuridik universiteti
Xalqaro xususiy huquq kafedrasi o‘qituvchisi
ORCID ID: 0000-0003-2217-6413
d.imamaliyeva@tsul.uz

ANNOTATSIYA

Global sog'liqni saqlash tizimlari hozirda tub o'zgarishlarni boshdan kechirmoqda. Biz tasavvur qilib bo'lmaydigan hajmdagi ma'lumotlarni yaratish va ulardan foydalanish imkoniyatini yaxshilash yo'lida katta o'tish davriga erishdik. Axborot inqilobi natijasida katta ma'lumotlarning paydo bo'lishi va rivojlanishi bilan biz endi ushbu ma'lumotni nazorat qilish usulini va sog'liqni saqlash sohasida kasalliklarni kuzatish va davolash qobiliyatini boshqarishimiz va o'zgartirishimiz mumkin. Boshqa tomondan, sog'liqni saqlash sohasida katta ma'lumotlarning paydo bo'lishi, ayniqsa shaxsiy ma'lumotlarning maxfiyligi, xavfsizligi, egalik qilish, boshqaruv va nazorat qilish bilan bog'liq qo'shimcha muammolarni keltirib chiqaradi. Ushbu maqola rozilik, anonimlashtirish, egalik qilish va ma'lumotlarni uzatish standartlari bo'yicha batafsil ob'ektiv orqali katta sog'liqni saqlash ma'lumotlarining huquqiy holatini tushunish uchun asos yaratadi.

Kalit so’zlar: *katta ma'lumotlar, maxfiylik, ma'lumotlarni anonimlashtirish, axloqiy standartlar, shaxsiy ma'lumotlar, transchegaraviy uzatish.*

ВВЕДЕНИЕ

В настоящее время глобальные системы здравоохранения претерпевают фундаментальные изменения. Мы достигли стадии серьезного перехода к

способам улучшения генерации и доступа к невообразимым объемам информации. С появлением и развитием больших данных в результате информационной революции мы теперь можем управлять и трансформировать подходы, с помощью которых мы контролируем эту информацию и, в здравоохранении, как следствие, способность контролировать и лечить болезни. С другой стороны, появление больших данных в здравоохранении создает дополнительные проблемы, особенно в отношении конфиденциальности личных данных, безопасности, владения, управления и контроля.

МАТЕРИАЛЫ И МЕТОДЫ

Юридические аспекты владения и контроля данных представляют собой сложный и непрерывно развивающийся алгоритм действий на сегодняшний день. В Республике Узбекистан существует единый законодательный акт, который регулирует конкретные аспекты защиты данных, например, Закон Республики Узбекистан «О персональных данных» 2019 года и Постановление Кабинета Министров Республики Узбекистан от 05.10.2022 г. № 570 «Об утверждении некоторых нормативно-правовых актов в области обработки персональных данных». Указанный закон, соответствующие постановления и приложения к ним предлагают комплексные правила в отношении данных, включающий обработку, согласие и трансграничную передачу данных. Кроме того, в качестве источника для изучения был взят Общий регламент по защите данных (GDPR) в Европейском Союзе, который имеет последствия для организаций, обрабатывающих данные граждан ЕС по всему миру. Поскольку Республика Узбекистан находится на этапе цифровой трансформации и выходит на глобальный рынок данных [1], понимание правовых аспектов, связанных с владением и контролем данных, становится решающим для обеспечения ответственного управления данными и защиты прав личности.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Правовой статус данных, связанных со здоровьем, является важнейшим компонентом более широкой правовой дискуссии о больших данных в здравоохранении. Обработка таких данных требует тщательного понимания их правового статуса, особенно в отношении согласия, анонимизации, владения данными и передачи данных.

Согласие

Данные, связанные со здоровьем, обычно относятся к категории конфиденциальных персональных данных, для сбора и использования которых

требуется явно выраженное согласие. Однако распространение больших данных усложняет процесс получения согласия из-за огромного масштаба и разнообразия обрабатываемых данных, что ставит под сомнение общепринятое понимание информированного согласия. Вопрос о том, достаточно ли существующих моделей согласия или следует разработать новые модели, адаптированные к большим данным, является активной областью юридических дискуссий.

Основным подходом, применяемым в исследованиях для уважения автономии людей, является получение информированного согласия. Основная цель процесса получения согласия в исследовании — обеспечить, чтобы пациенты поняли цель, риски и методологию проводимого исследования [2]. Процесс получения согласия поддерживает этические принципы автономии и свободы выбора, позволяя пациентам сделать вполне обоснованное решение по выбору. Хотя процесс получения согласия, возможно, несовершенен и ограничен, он является лучшим доступным инструментом для соблюдения вышеупомянутых этических принципов [3]. Однако, учитывая, что исследования больших данных радикально отличаются от традиционных исследований с точки зрения участия субъектов, одна из самых больших проблем заключается в том, представляют ли текущие требования к исследованиям в отношении согласия по-прежнему адекватную защиту автономии пациентов. Новые стандарты подчеркивают важность надлежащего согласия, требуя от исследователей кратко изложить пациентам то, что им нужно знать относительно того, почему они хотят или не хотят участвовать в протоколе, что является самым началом каждого документа об информированном согласии [4].

Однако, использование больших данных не во всех обстоятельствах предусматривает наличие согласия на широкий круг данных, и впоследствии, отсутствие согласия означает, что участникам не предоставляется полное понимание использования их данных. Проблема согласия с широким спектром заключается в том, что в отличие от документов об информированном согласии, которые предназначены для конкретного проекта или исследовательского использования, документы о широком согласии носят более общий характер и относятся к неопределенному диапазону будущих научных исследований. Данная неопределенность относительно того, как будет использоваться информация значительно усложняет принятие обоснованного решения об участии в исследовании. Помимо опасений по поводу широкого согласия, существуют также опасения по поводу отсутствия согласия. Когда

исследователи больших данных используют обезличенную общедоступную информацию, для которых согласие участников исследования не требуется. Беря во внимание, что информация, используемая в исследованиях больших данных, часто создается отдельными лицами для целей, отличных от исследований, люди, вероятно, могут не быть осведомлены о потенциальном использовании их персональной информации [5]. Существующие на сегодняшний день модели согласия не рассматривают в полной мере условия, в которых создается информация, используемая в исследованиях больших данных.

Отсутствие более строгих требований к согласию на общедоступную информацию порождает опасения по поводу автономии, поскольку лица, генерирующие эти данные, часто не осознают, в какой степени их информация является общедоступной. Более того, люди могут не осознавать, в какой степени их информация может быть использована другими без их разрешения или какие выводы можно сделать на основе анализа их данных. Это может легко произойти, когда исследователи получают свои наборы данных непосредственно из Интернета через такие платформы, как, например, социальные сети. Веб-сайты, которые исследователи больших данных используют в качестве источников информации, часто служат неотъемлемой частью повседневной жизни людей, и значительная часть людей могут считать свою информацию конфиденциальной, несмотря на ее доступность [6]. Например, когда кто-то публикует в Facebook информацию о болезни, даже если он решил сделать свой профиль доступным для просмотра другими, он может ожидать, что его конфиденциальную публикацию увидят только те, кто связан с его кругом общения. Мало того, что они могут ожидать, что публикацию увидит только их круг общения, они также могут ожидать, что никто не будет использовать эту публикацию. Действующие правила проведения исследований определяют общественную и частную информацию на основе доступности. Это не обязательно соответствует тому, как участники определяют общественную и частную информацию.

Анонимизация

Методы анонимизации играют ключевую роль в защите конфиденциальности при использовании больших данных в здравоохранении. К примеру, GDPR способствует псевдонимизации и анонимизации персональных данных [7]. Однако сохраняются опасения по поводу потенциальной повторной идентификации лиц по предположительно

анонимным данным, проблема усугубляется в контексте больших данных из-за повышенной вероятности непредвиденных связей данных [8].

Анонимизация — это средство предотвращения нарушения конфиденциальности и сохранения конфиденциальности. Анонимизированные данные не защищены законом о защите данных. Конфиденциальность и неприкосновенность частной жизни — взаимосвязанные понятия: конфиденциальность — это обязанность, которую часто несет профессионал перед лицом в определенных обстоятельствах; неприкосновенность частной жизни – это право, которым пользуется человек. Человек раскрывает множество конфиденциальных фактов профессионалам, особенно в области права и медицины [9], понимая, что у профессионала есть профессиональная, юридическая и этическая обязанность сохранять конфиденциальность информации и данных, иначе он столкнется с серьезными санкциями за нарушение этих обязанностей [10]. Обязанность конфиденциальности не применяется, если данные были анонимизированы. Обязанность конфиденциальности включена в Клятву Гиппократа и Женевскую декларацию, однако в Женевской декларации есть дополнительная обязанность: «делиться своими медицинскими знаниями на благо пациента и для улучшения здоровья пациентов».

Этот запрет можно интерпретировать как возложение на врачей обязанности делиться данными для целей медицинских исследований, проводимых ради общего блага. В Великобритании Управление комиссара по информации (ICO) и Caldicott Review прокомментировали проблему неиспользования данных [11]. Калдикотт сделал это дополнительным седьмым принципом: «Обязанность делиться информацией может быть столь же важной, как и обязанность защищать конфиденциальность пациентов». Хотя этот дополнительный принцип относится к конкретным обязанностям человека, а не к исследованиям как таковым, его можно интерпретировать как включающий обязанность использовать данные для улучшения медицинского обслуживания.

Различие между неприкосновенностью частной жизни и конфиденциальностью признается в законе о защите данных, в котором особые меры защиты применяются к тем, «кто в данных обстоятельствах несет обязанность соблюдать конфиденциальность, эквивалентную той, которая возникла бы, если бы это лицо было медицинским работником» (Закон Великобритании о защите данных). 1998 г.; аналогичные положения применяются и в других транспозициях Директивы о защите данных. Безопасные убежища для данных требуют от исследователей контрактной

обязанности сохранять конфиденциальность и не предпринимать попыток повторной идентификации. Серьезные санкции следует применять только к тем, кто намеренно нарушает руководящие принципы; в противном случае возникнет тенденция излишне ограничивать обмен данными [12].

Владение данными и их передача

Вопрос о праве собственности на данные остается юридически спорным. Отсутствие универсальной правовой базы, которая четко определяет право собственности на данные, оставляет этот вопрос предметом регулирования различных национальных законодательств, договорных соглашений и этических соображений. В контексте здравоохранения юридическое определение права собственности на данные (будь то субъект данных, поставщик медицинских услуг или третья сторона) существенно влияет на управление данными и распределение прав и обязанностей в отношении использования данных.

Передача данных, особенно международная, является еще одним важным юридическим аспектом. Трансграничная передача персональных данных строго регулируется международными законами, такими как GDPR, в первую очередь из-за соображений конфиденциальности [7]. В контексте здравоохранения эти правила имеют серьезные последствия для глобального сотрудничества в области исследований в области здравоохранения, многонациональных поставщиков медицинских услуг и компаний цифрового здравоохранения, работающих в нескольких юрисдикциях.

Сложный правовой статус данных, связанных со здоровьем, подчеркивает необходимость всестороннего правового понимания и надежной нормативно-правовой базы, обеспечивающей защиту конфиденциальности и этическое обращение с данными при реализации огромного потенциала больших данных в здравоохранении. Подробный юридический анализ должен быть сосредоточен на таких ключевых областях, как защита данных, правила конфиденциальности, права интеллектуальной собственности, рамки ответственности и этические соображения. Изучение правовых подходов других стран позволит Узбекистану выявить пробелы в существующей законодательной базе и принять меры по развитию ответственного использования технологий при защите прав и интересов физических и юридических лиц, участвующих в сфере здравоохранения. Проведя всесторонний и углубленный правовой анализ, Узбекистан сможет разработать надежную правовую основу, которая позволит решить проблемы и возможности, связанные с интеграцией технологий в здравоохранение.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ (REFERENCES):

1. Указ Президента Республики Узбекистан «Об утверждении стратегии «Цифровой Узбекистан-2030» и мерах по ее эффективной реализации» от 05.10.2020 г. № УП-6079 // Национальная база данных законодательства, 11.11.2023 г., № 06/23/193/0844
2. Paterick TJ, Carson GV, Allen MC, Paterick TE. Medical informed consent: General considerations for physicians. Mayo Clin Proc. 2008;83(3):313–319.
3. Abujarad F, Alfano S, Bright TJ et al. Building an informed consent tool starting with the patient: The patient-centered virtual multimedia interactive informed consent (VIC). AMIA Annu Symp Proc. 2017;2017:374–383.
4. Menikoff J, Kaneshiro J, Pritchard I. The common rule, updated. N Engl J Med. 2017;376(7):613–615.
5. Vayena E, Mastroianni A, Kahn J. Caught in the web: Informed consent for online health research. Sci Transl Med. 2013.
6. Mittelstadt BD, Floridi L. The ethics of Big Data: current and foreseeable issues in biomedical contexts. Sci Eng Ethics. 2016;22(2):303–341.
7. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj
8. Rocher, L., Hendrickx, J.M. & de Montjoye, YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019)
9. Carman D, Britten N. Confidentiality of medical records: the patient's perspective. Br J Gen Pract. 1995 Sep;45(398):485–8.
10. Sankar P, Mora S, Merz J, Jones N. Patient perspectives of medical confidentiality: a review of the literature. J Gen Intern Med. 2003 Aug;18(8):659–69.
11. Information Commissioner's Office . Anonymisation Code. London: Information Commissioner's Office; 2018-09-05. Anonymisation: managing data protection risk code of practice Internet https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.
12. Laurie G, Jones K, Stevens L, Dobbs C. Report. London: Nuffield Council on Bioethics/Wellcome Trust; 2014. A Review of Evidence Relating to Harm Resulting from Uses of Health and Biomedical Data.