БОЛЬШИЕ ОБЪЕМЫ ДАННЫХ И ЗДОРОВЬЕ – СУВЕРЕНИТЕТ ДАННЫХ КАК СРЕДСТВО ФОРМИРОВАНИЯ СВОБОДЫ ИНФОРМАЦИИ

Deutscher Ethikart[1]

BIG DATA AND HEALTH – DATA SOVEREIGNTY AS THE SHAPING OF INFORMATIONAL FREEDOM

Opinion – Executive summary & Recommendations
30 ноября 2017 г.

Основные принципы: Большие объемы данных и здоровье

(1) Большие данные являются одним из ключевых терминов в современных дискуссиях о социальных изменениях, обусловленных технологиями. Это относится к обработке больших объемов данных с целью выявления различимых принципов и, таким образом, получения новых идей. Объем и разнообразие данных, а также скорость, с которой они собираются, анализируются и взаимодействуют, требует использования инновационных и постоянно меняющихся технологических подходов.

(2) С самого начала современного периода систематический сбор и анализ данных представляет собой важный фактор развития цивилизации и охватывает как людей, так и окружающую их среду, например, в области биологии и медицины, психометрии, эпидемиологии и социальных наук, Использование современных компьютеров, технологий хранения данных и высокоскоростных сетей привело к значительному увеличению объема доступных данных. Это также способствовало различным качественным достижениям, таким как использование все более сложных наборов инструкций по обработке (алгоритмов) в компьютерном моделировании, требующем интенсивной работы процессоров, а также рационализации, стандартизации и уточнения многочисленных рабочих процессов.

(3) Разработка больших структур данных влечет за собой трансформацию каждого этапа обработки информации, характеризующуюся усилением автоматизации обработки данных и взаимосвязи, и взаимопроникновения данных. Как объем, так и скорость полностью автоматизированного сбора данных за последние несколько лет экспоненциально увеличились, а быстрое распространение и создание сетей растущего числа устройств, способных собирать данные во всех сферах повседневной жизни, постоянно открывает новые источники данных.

(4) Это особенно заметно в секторе здравоохранения, где растущее число исследователей, компаний и врачей использует информацию, полученную в результате обработки огромных количеств данных. Кроме того, генерация данных, относящихся к здоровью людей, например, с помощью приложений для смартфонов и датчиков, надеваемых на тело, постоянно растет. Взаимосвязь и анализ этих разнообразных данных дает возможность

[1] Этическое общество Германии – некоммерческая организация, основанная в 2008 г.

понять состояние здоровья, характер личности и образ жизни человека, даже учитывая прогнозы, касающиеся, например, развития болезни.

(5) Как только данные собираются, производится обмен ими и взаимосвязь, часто через государственные границы, а иногда и в реальном времени - сетями передачи данных и сетевыми программными системами. Для достижения этой цели разрабатываются технические стандарты для обмена данными через интерфейсы прикладного программирования (API). Это также облегчает установление правил использования данных и отслеживание данных.

(6) Для эффективного сбора, хранения и обработки данных требуются мощные компьютеры. Эти данные часто предлагаются коммерческими провайдерами, их потенциальная возможность обычно обеспечивается центрами обработки данных, содержащими многочисленные сетевые серверы. Переход от локальных компьютеров к виртуальному пространству центров обработки данных привел к появлению облачных вычислений.

7) Объективность, надежность, возможность воспроизводимости и обоснованность используемых данных и методов анализа являются ключевыми факторами для оценки любых заявлений, выводов или прогнозов на основе этих данных. По мере увеличения количества данных также учитывается значение анализа для отдельных факторов, а также способность учитывать дополнительные факторы и их взаимодействия, даже те, которые имеют только слабые эффекты. Тем не менее независимый обзор и проверка анализа данных по-прежнему имеет центральное значение.

(8) Статистические отношения между переменными (корреляциями) не могут служить основой для выводов относительно причин (случайных эффектов) или способов действий. Они могут быть выяснены только посредством дополнительных аргументов и предположений или с помощью дополнительных данных, например, полученных при долгосрочных или экспериментальных исследованиях.

(9) Машинное обучение имеет особое значение для использования и дальнейшей разработки приложений с большим объемом данных. Здесь с помощью обучающих наборов данных статистические модели "изучают" алгоритмы, которые позволяют классифицировать или группировать данные определенным образом. Главный вопрос, который поднимает этот вопрос, касается степени, в которой такие методы могут привести к появлению машинных агентов[2] со способностью и полномочиями принимать решения, которые могут вмешиваться, например, в формирование политики лечения или здравоохранения.

(10) Используя данные, полученные от большого числа людей, системы самообучения могут различать важные факторы, такие как поведение, связанное со здоровьем, и могут находить отдельных лиц и ценности в рамках этой системы координат. Такие подходы могут быстро готовить индивидуальные рекомендации и разрешать индивидуальные взаимодействия с машинами-операторами помощниками. Однако они также обязательно приводят к разглашение личной информации и увеличивают возможности для обмана и манипулирования личными решениями.

(11) Анализируя связи между разрозненными данными наблюдений, методы обработки, при которых используют большие объемы данных, способны выявлять все более тонкие различия между людьми. Таким образом, сугубо

[2] Программа, самостоятельно выполняющая задание, указанное пользователем компьютера, в течение длительных промежутков времени.

личные характеристики и обстоятельства все чаще влияют на процессы принятия решений - например, в отношении медицинской диагностики, прогнозов и лечения или в присвоении страховой системой страхователям различных категорий страховых премий. Однако при использовании сложных алгоритмов больших данных для создания таких групп (стратификация) необходимо учитывать и минимизировать любые потенциальные источники ошибок.

(12) Данные, связанные со здоровьем, которые могут быть отнесены к конкретному человеку, особенно чувствительны, поскольку позволяют проникнуть в чрезвычайно интимную сферу. Такие индивидуальные данные могут быть зафиксированы, и они связаны с постоянно растущим числом источников. В ходе их анализа даже данные, которые на первый взгляд кажутся случайными, такие как информация, относящаяся к перемещению кого-либо или поведению в магазине, могут быть определены как имеющие отношение к оценке своего здоровья.

(13) Данные, относящиеся к здоровью, накапливаются в различных, частично перекрывающихся контекстах: от медицинской практики и исследований, связанных со здоровьем, до правительственных учреждений и страховых компаний, включая активное или непреднамеренное получение данных пациентами и самими гражданами. Кроме того, технологии с большим объемом данных облегчают тщательную деконтекстуализацию3 и реконстектуализацию4 данных, собранных, проанализированных и перекомпонованных для разных целей. Это приводит к размыванию границ в отношении того, что может считаться относящимся к здоровью; это также увеличивает вероятность того, что данные могут быть де-анонимизированы[5], или отдельные лица будут повторно идентифицированы.

(14) Поскольку все данные, независимо от формы, в которых они генерируются, могут быть истолкованы как связанные с личным здоровьем, в принципе, можно классифицировать все такие данные как важные для здоровья. В результате такого развития ситуации часто невозможно определить во время сбора данных, следует ли считать некоторые данные чувствительными или важными для здоровья. Скорее, это зависит прежде всего от контекста, в котором используются данные. Этот контекст может меняться со временем.

(15) Различные участники с различными функциями и, по крайней мере, частично противоположными интересами, работающие в различных обстоятельствах, несут ответственность за сбор, обработку и использование огромных объемов данных. Здесь можно выделить пять областей, в которых большие объемы данных применяются в отношении здоровья, и которые рассматриваются как образцовые, рассматриваются с точки зрения потенциальных преимуществ и рисков: во-первых, биомедицинские исследования; во-вторых, предоставление медицинских услуг; в-третьих, использование данных страховщиками и работодателями; в-четвертых, коммерческое использование данных, относящихся к здоровью, глобально работающими ИТ и интернет-компаниями; и, в-пятых, сбор таких данных подвергшимися заболеванию лицами.

---

[3] Интерпретация текста, беседы, полностью основанная на дословном значении материала, т.е. игнорирующая контекст.

[4] Реконтекстуализация – процесс, при котором извлекается текст, знаки или значения из исходного контекста, чтоб ввести его в другой контекст

[5] Деанонимизация – нарушение анонимности, заключающееся в публикации персональных данных участника Интернета.

(16) В биомедицинских исследованиях (первая область) анализ больших объемов данных, имеющих отношение к здоровью, призван способствовать улучшению понимания научно важных связей и процессов. Среди наиболее информационно емких для данных применений - современные визуализационные обследования и молекулярно-биологические процедуры, такие, которые используются в так называемых "омиках[6]" (например, геномика[7], протеомика[8], метаболомика[9]).

(17) Основными участниками биомедицинских исследований являются не только научно-исследовательские институты и их сотрудники, но и предметы исследований и пациенты. Использование больших объемов данных в исследованиях в целом соответствует высоким и хорошо поддающимся проверке стандартам сбора, использования и безопасности данных и часто связаны с участием нескольких учреждений. Научные организации используют новые технические и инфраструктурные возможности больших данных, объединяются друг с другом, чтобы обмениваться данными и сотрудничать в их анализе и оценке.

(18) Взаимодействие факторов, которые вызывают и модулируют многие заболевания, чрезвычайно сложны. Большие объемы данных позволяют исследователям интегрировать и объединить различную информацию из разных источников в рамках комплексного анализа. Не только общий объем данных важен для такой операции, но и качество их интерпретации.

(19) Объединение данных, собранных различными учреждениями в очень разных обстоятельствах, создает особые проблемы для использования больших объемов данных в медицинских исследованиях. аннотации и контроля качества; так же хорошо функционируют правила обмена данными. Это связано, с одной стороны, с опасениями по поводу защиты персональных данных и нехваткой подходящих каналов для общения и моделей для получения согласия пациентов и субъектов исследования относительно вторичного использования данных. С другой стороны, существуют неопределенность и различные точки зрения относительно вопроса о том, кто имеет право на доступ к данным, полученным в результате исследований, и в какой степени.

(20) Наряду с новыми моделями для получения согласия пациента или субъекта потенциальные решения в этой области включают, в частности, технические меры по стандартизации обмена данными, которые гарантируют качество данных и высокие стандарты защиты частной жизни, а также нормативную поддержку и инициативы по содействию открытому обмену данными.

(21) В области предоставления медицинских услуг (область два) использование больших объемов данных дает возможности для разработки более персонализированных планов лечения, а также для повышения эффективности и действенности. Опираясь на большой объем данных, можно уточнить распределение пациентов по группам, чтобы, например, уменьшить побочные эффекты и избежать ненужных методов лечения. Сбор и оценка

---

[6] Омики – направления биологической науки, рассматривающие всю совокупность соответствующих объектов организма структурно-функциональной взаимосвязи.
[7] Раздел молекулярной генетики, изучающий геномы и гены живых организмов.
[8] Область молекулярной биологии, посвященная идентификации и количественному анализу белков.
[9] Систематическое изучение уникальных химических "отпечатков пальцев", специфичных для процессов, протекающих в живых клетках.

данных, связанных с здоровьем, также открывает новые возможности для раннего выявления и профилактики заболеваний.

(22) Сектор здравоохранения характеризуется множеством субъектов с частично расходящимися интересами. К ним относятся поставщики медицинских услуг, страховщики и пациенты, а также правительства, группы интересов и исследователи, которые непосредственно участвуют в клинической практике.

(23) Наряду с возможностями, представленными подходами с интенсивным использованием данных, существуют также риски для пациентов, которые отказываются от контроля своих собственных данных и сталкиваются с тем, что поставщики услуг здравоохранения все чаще проникают в самую интимную сферу ("прозрачный пациент"), наряду с повышенным риском злоупотребления данными. К этим рискам можно добавить опасения, что растущее использование подходов к медико-санитарной помощи, основанное на больших объемах данных, может еще больше снизить личное внимание медицинских работников, которые они посвящают своим пациентам, и что их некритическое или неправильное применение может привести к ошибкам в диагностике и лечении.

(24) Для работодателей и страховщиков (третья область) большие объемы данных предоставляют широкие возможности для доступа и анализа ценной информации, и это та область, в которой не всегда в достаточной мере соблюдаются действующие законодательные положения. Непрерывно растущие объемы данных и новые способы связывания этих данных позволяют получать более подробные характеристики отдельных лиц или групп людей.

(25) Это привело к возникновению опасений относительно возможности дискриминации с учетом вероятных сценариев, в которых страховщики и работодатели, анализируя коммерчески доступные личные поведенческие характеристики, созданные с использованием больших объемов данных, могут селективно выбирать только претендентов или кандидатов с низким уровнем риска или предлагать им лучшие условия.

(26) Даже при существующих контрактах работодатели и страховщики кровно заинтересованы в нормальном состоянии здоровья своих сотрудников и страхователей, поскольку болезнь может вызывать значительные издержки. Мониторинг поведения пациента или сотрудника позволяет ввести стимулы для поощрения здорового образа жизни или санкции, чтобы препятствовать нездоровому образу жизни. Поскольку такие программы приводят к снижению заболеваемости, они предлагают привлекательные перспективы для всех участников. Однако риски нельзя игнорировать. Ни корректировка страховых премий, ни дисциплинарные предупреждения, полученные за поведение, наносящее ущерб здоровью, не отвечают интересам тех, кто делится своими данными о состоянии здоровья.

(27) Глобальные ИТ-компании и интернет-компании (четвертая область) в основном выполняют роль поставщиков услуг. На основе их доступа к огромным количествам данных и управлением необходимой инфраструктурой данных они могут предоставлять поисковые системы, интерактивные информационные платформы и такие предложения, как покупки через интернет-магазины, а также широкий спектр многофункциональных устройств. Таким образом, многочисленные пользовательские данные собираются в широких масштабах, хранятся и используются. Для таких компаний, которые все активнее действуют в областях, имеющих отношение к здравоохранению, таким образом однозначно можно связать данные, относящиеся

прежде всего к здоровью, с многочисленными другими видами информации. Это подразумевает большую возможность злоупотреблений.

(28) Компании предлагают программное обеспечение, аппаратное обеспечение, разработку технологий и онлайн-услуги для приложений с большим объемом данных. Они предоставляют институтам, ориентированным на данные, доступ к системам, алгоритмам, устройствам и инфраструктуре для сбора, анализа, управления и хранения данных; цель заключается в ускорении и совершенствовании процессов и обеспечении высокоэффективного использования соответствующей информации.

(29) Рост активности цифровых фирм в секторе здравоохранения открывает возможности для исследований и медицины: по сравнению с государственным сектором крупные интернет-компании имеют доступ к значительно большему объему данных и часто оснащены лучшими техническими и финансовыми ресурсами, а также более мощными средствами анализа данных. С другой стороны, ограничивая доступ к данным для тех, кто первоначально предоставил данные, или для тех, кто заинтересован в использовании этих данных для медицинских или исследовательских целей, частные фирмы также могут потенциально препятствовать медицинскому прогрессу.

(30) Сбор данных, относящихся к здоровью, для самих страдающих заболеваниями лиц (пятая область) облегчается многочисленными носимыми устройствами с датчиками и приложениями, с помощью которых все больше данных о здоровье, деятельности и окружающей среде человека собирается, обрабатывается и объединяется с существующими запасами данных. Более того, перевод в цифровую форму явления повседневной жизни продвинулся до такой степени, что обычное поведение и формы коммуникации автоматически влекут за собой создание данных - зачастую даже выходящих за рамки социальных сетей, приложений для жизни и подобных услуг.

(31) Устройства и приложения, которые собирают данные, относящиеся к здоровью, могут облегчить пользователям доступ к собственной информации о здоровье независимо от времени или места и могут облегчить предоставление медицинских услуг, основанных на фактических данных. Они также могут способствовать здоровому образу жизни и дальнейшему личному благополучию. Кроме того, они предлагают возможность расширения исследований при использовании в качестве важного количественного и качественного дополнения к существующим данным.

(32) С другой стороны, чрезмерный режим самоконтроля, который характерен для таких услуг и устройств, может способствовать преувеличенному стремлению к оптимизации, пагубному для личного здоровья, а также к медикализации[10] "естественных" жизненных процессов. Кроме того, возникает вопрос о том, является ли самоотслеживание действительно выражением личного суверенитета или же оно представляет собой форму самопроизвольной обособленности. Также вызывает обеспокоенность возможность дискриминации в отношении лиц, неспособных или не желающих подвергать себя таким исследованиям. Тот факт, что многие приложения и устройства для самостоятельного отслеживания ориентированы на экономические интересы своих производителей, наряду с неадекватными

[10] Медикализация – процесс, во время которого человеческое состояние и проблемы начинают определяться и рассматриваться как медицинские состояния и проблемы, и таким образом, попадают в сферу влияния и власти врачей для изучения, диагностики и лечения.

удобствами для пользователя, прозрачностью и защитой конфиденциальности, которые многие демонстрируют, также стали причиной критики.

(33) Таким образом, можно идентифицировать следующие сильные стороны, слабые стороны, возможности и риски в отношении растущего наличия больших объемов данных в областях, важных для здоровья, независимо от контекста приложений. Сильные стороны включают растущий размер баз данных и связанная с ними разработка инновационных цифровых инструментов, а также высокий уровень взаимодействия участников. К недостаткам относятся несоответствия качества данных, отсутствие прозрачности потоков данных и потеря контроля над данными, а также повышенные требования к контролю, регулированию и квалификации.

(34) Перспективы, связанные с большими объемами данных, состоят прежде всего в улучшении возможностей разделения на группы в диагностике, лечении и профилактике, в результате чего повышаются эффективность и действенность, а также поощряется поведение, способствующее укреплению здоровья. Риски возникают из-за размывания принципов и практики социальной солидарности, распространения ответственности, монополизации, неправильного использования данных и информационной преступности.

(35) Однако, как судить о конкретных важных для здоровья применениях данных, зависит от ключевой степени вовлеченных сторон, их различных интересов, их собственных оценок риска и возможностей, а также конкретного контекста применения.

Правовые положения, касающиеся большого объема данных

(36) Большие объемы данных представляют собой серьезную проблему для правовой системы. Особое значение в этом отношении имеют государственное право, общее законодательство о защите данных и специальные положения о защите данных, относящиеся к сектору здравоохранения, а также нормативные положения о медицинских устройствах, а также основные механизмы стимулирования и механизмы саморегулирования и комбинированного управления.

(37) Ключевые элементы закона о защите данных составляются на уровне Основного закона Германии. Основным конституционным стандартом на национальном уровне является право на информационное самоопределение[11], принцип, разработанный Федеральным конституционным судом, в его примечательном суждении об участии в переписи как конкретное воплощение общего права личности. Он поддерживает и расширяет конституционную защиту неприкосновенности частной жизни и свободы поведения[12].

(38) Конституционное право свободного развития самого человека может столкнуться с вопросами, вызывающими озабоченность в отношении общего блага, такими как продвижение научного прогресса или обеспече-

[11] Термин информационное самоопределение впервые был использован в контексте решения Конституционного суда Германии относительно личной информации, собранной в ходе переписи 1983 г.: в контексте современной обработки данных, защита индивидуума от неограниченного сбора, хранения, использования и раскрытие его личных данных гарантируется общими правами личности, изложенными в Конституции.

[12] В праве свобода – это закрепленная в Конституции или ином законодательном акте возможность определенного поведения человека (например, свобода слова, свобода вероисповедования и т.д.)

ние эффективного и адекватного медицинского обслуживания. Конфликты могут также возникать с основополагающими правами других частных субъектов, которые хотят иметь доступ и использовать имеющиеся у них данные.

(39) Закон о защите данных ориентирован на эти конституционные положения. Тем не менее, он применяется во многих обстоятельствах, которые появились только в результате новых технических разработок и для которых он изначально не был разработан. Даже самые последние поправки, принятые в соответствии с Европейским стандартом защиты данных (GDPR), не сделали его достаточно приспособленным к появлению больших объемов данных. Это применимо, несмотря на явный прогресс, который эти новые положения представляют с точки зрения, например, установления трансграничных стандартов или более пристального внимания к концепции конфиденциальности по определению.

(40) Основополагающие допущения, ведущие принципы и цели традиционного законодательства о защите данных вряд ли могут быть согласованы с уникальными характеристиками приложений для больших объемов данных. Основные принципы традиционного законодательства о защите данных - определения, касающиеся личного характера данных, приемлемого использования данных и обязательства соблюдать их, необходимость, соразмерность и минимизация сбора данных, необходимость согласия и прозрачности - противостоят особой логика больших объемов данных. Если мы не просто хотим ввести общий запрет на использование больших объемов данных, и в то же самое время отказываемся принять значительные ограничения в защите, которые он влечет за собой, тогда мы должны разработать новые формы регулирования и способы формирования событий в этой области.

(41) В соответствии с этим закон о защите данных относится к личному характеру данных и делает особый акцент на необходимости его использования, чтобы он оставался конкретным для намеченной и определенной цели. Однако характер больших объемов данных заключается в том, что будущее использование данных, которые могут быть собраны, не предсказуемо на момент их сбора, и что связь между данными и лицом или состоянием его здоровья определяется только, по крайней мере, при определенных обстоятельствах, после события. Данные, которые были сохранены для одной цели, часто анализируются в связи с другой целью, или данные просто собираются для еще неопределенных целей.

(42) Кроме того, большие объемы данных, очевидно, несовместимы с принципом экономии данных или минимизации, в соответствии с которым необходимо как можно меньше собирать, обрабатывать или использовать личные данные. Если он будет полностью применен, этот принцип легко приведет к далеко идущему аннулированию возможностей, представленных большим объемом данных. Поскольку потенциальная опасность для права на информационное самоопределение увеличивается пропорционально объему хранимых данных, необходимы, однако, более эффективные механизмы защиты данных.

(43) Очевидно, что большие объемы данных несовместимы с обязательством получения согласия, в соответствии с действующим законодательством о защите данных, в соответствии с которым использование данных разрешено только при условии согласия лиц, затронутых в полной мере с учетом характера и объема предполагаемого использования данных. Даже в том, что касается этого, есть веские основания сомневаться в том, что лица, поставляющие данные, полностью осознают характер использования их данные, и последствия такого использования. Большие объемы данных зна-

чительно осложняет эту общую проблему, так как будущее использование данных часто просто неизвестно в момент сбора этих данных.

(44) Более того, за пределами согласия существующий закон о защите данных предлагает лишь несколько возможностей влиять на дальнейшую судьбу данных. Каждое дальнейшее использование требует своего предоставления согласия, и как только данные собираются с согласия, они больше не могут отслеживаться теми, кого это затрагивает. Динамика больших объемов данных не соответствует этой нормативной модели. Особенно, если рассматривать согласие затронутых лиц как основополагающее требование защиты данных, следует изучить новые пути, с помощью которых это было бы возможно, и технически необходимо в условиях больших объемов данных.

(45) Кроме того, вследствие сочетания и взаимосвязи различных данных большие объемы данных увеличивают шансы на повторную идентификацию и подрывают эффективность требований скрытия личной информации и псевдонимизации[13]. В какой степени и в какой момент существует опасность того, что повторная идентификация анонимных данных, взятых в отдельности, будет оправдывать предположение, что эти данные подлежат защите как имеющие личный характер? Этот вопрос только добавляет проблемы, связанные с уже оспариваемой концепцией персональных данных в законе о защите данных.

(46) Право быть информированным при сборе личных данных, а также право на их исправление, удаление и блокирование служит обеспечению прозрачности, но часто обеспечивает небольшую эффективную защиту. Особенно в контексте больших объемов данных лица, поставляющие данные, вряд ли смогут идентифицировать все потенциальные стороны, в отношении которых могут быть выставлены претензии. Более того, требование о том, чтобы способы обработки данных были понятны тем, кто предоставил их, что охватывает право на информацию, оказывается сложным для реализации в свете сложных и самообучающихся алгоритмов, используемых большими объемами данных. Таким образом, право на исправление и удаление аннулируется, поскольку затронутые лица не могут воспользоваться этими правами, не будучи в полной мере проинформированы о своих данных.

(47) Этот анализ недостатков общего законодательства о защите данных также может быть применен с определенными ограничениями к специальной области законодательства о защите данных о здоровье. Последнее дополняет закон о защите данных, который часто адаптируется к конкретным областям применения, с гражданскими, уголовными и профессиональными правовыми положениями, касающимися конфиденциальности пациентов. В конечном счете, однако, возможные решения, предлагаемые законом о защите данных здравоохранения, также в значительной степени оказались в ловушке понимания проблемы, предшествующей появлению больших объемов данных.

(48) Положения законодательства о медицинских устройствах, которые направлены на регулирование свободной торговли медицинскими приборами, гарантируя безопасность, пригодность и эффективность таких устройств для защиты пациентов, пользователей и третьих лиц, могут иметь компенсирующий эффект. В отличие от медикаментов, медицинские уст-

[13] Псевдонимизация – замена имени или какого-либо другого идентификационного признака участника разговора на псевдоним.

ройства не требуют одобрения правительства, но тем не менее должны быть сертифицированы в соответствии с оценкой риска для конкретного продукта, минимизацией рисков и анализом рисков/выгод, а также оценкой соответствия, соответствующей рискам, присущим продукту.

(49) Программное обеспечение, которое служит медицинским целям, может быть классифицировано как медицинское изделие. Независимо от того, зависит ли это от объема информации, предоставленной производителем. На практике, однако, различие между медицинскими применениями и простыми применениями для жизни или хорошего физического состояния часто бывает трудно провести.

(50) Положения закона о медицинском страховании также имеют отношение к большим данным. Включая затраты на приложения мобильных медицинских услуг в своем страховом покрытии, частные и действующие по закону страховщики могут, например, создавать финансовые стимулы для разработчиков этих продуктов, а также предлагать альтернативу модели "платы за предоставляемые данные". Однако остается доказать, будет ли это эффективным подходом. Кроме того, следует избегать опасности дискриминации, в том числе в отношении использования таких данных при определении страховых премий.

(51) В свете недавней, всесторонней реформы закона о защите данных через GDPR и новой версии Федерального закона о защите данных, еще предстоит выяснить, действуют ли, и как именно новые правила и механизмы в этой области. Тем не менее, очевидно, что многие из основных принципов действующего законодательства о защите данных практически не согласуются с концепцией больших объемов данных. Гибкие нормативы, открытые для инноваций и действующие в рамках относительной свободы действий, предусмотренной конституционным правом, могут учитывать эту специфическую напряженность наряду с потенциальным использованием комплексных, гражданско-правовых и кооперативных регулирующих актов гражданского статуса.

(52) Особое значение имеет то, чтобы выяснить, в какой степени отсутствие конкретности, которая характеризует важные для здоровья приложения с большими объемами данных, может быть компенсировано дополнительными техническими и организационными, а также материальными и процедурными гарантиями. Поскольку закон о защите данных продолжает совершенствоваться, это, прежде всего, более полностью дифференцированная модель согласия, предоставляющая возможности для конкретных особенностей регулирующей области и предпочтений затронутых лиц, или ужесточение правил сбора и использования данных на основе правовых санкций, которые возникают в этом отношении. Гражданское право также будет играть важную роль в развитии защиты данных, особенно в области закона о защите прав потребителей, законодательства об ответственности и правил, касающихся присвоения владения данными и полномочий определять их использование (владение данными).

(53) Все нормативные подходы к большим объемам данных должны сталкиваться с проблемой реагирования на глобальное по сути явление с юридическим аппаратом территориально ограниченного государства. Существующие законы о защите данных, рассматриваемые на международном уровне, широко варьируются, представляя, как тех, кого затрагивают большие объемы данных, так и тех, кто стремится регулировать их в рамках уникальных проблем. Несмотря на многочисленные усилия по согласованию мер защиты

данных, многочисленные практические препятствия по-прежнему препятствуют эффективному международному применению закона.

(54) В свете специфической динамики и непостоянства этой регулирующей области предлагаются совместные решения, разработанные за пределами полномочий государственной власти, такие как сертификация продуктов с защитой данных или защитой данных с помощью пароля, или разработка кодексов корпоративной этики или передовой практики в науке и в частном секторе.

Этика больших объемов данных и здоровья

(55) Большие объемы данных влияют как на этические рамки, которые нормативно и описательно связаны с ролью, функцией и положением индивидуума, осуществляющего передачу данных, так и на основные направления социальной ориентации. К соответствующим концепциям относятся свобода и самоопределение, неприкосновенность права личной и интимной жизни, суверенитет и полномочия, милосердие и не причинение вреда, а также справедливость, солидарность и ответственность.

(56) Понятие свободы используется по-разному. Различие между авторством своих действий как основным условием свободы, с одной стороны, и самоопределением, как практическим воплощением свободы, в зависимости от более или менее отчетливо воспринимаемых обстоятельств, с другой стороны. Авторы действий могут быть в определенной степени независимы.

(57) Концепция самоопределения относится к способности человека формировать свою жизнь в соответствии со своими собственными идеями, а также фактическим воплощением этой способности и идеальным способом вести свою жизнь. Эти формы личного самоопределения должны быть дифференцированы от правовой защиты, обеспечивающей их осуществление. Практическое значение имеют способы осуществления самоопределения и степени, в которой это происходит. Таким образом, в определенных обстоятельствах можно делегировать свое право на самоопределение или частично компенсировать ограничения на способность к самоопределению через представителей.

(58) В контексте больших объемов данных в последние годы особенно заметно было развитие новых моделей хранилищ биологических материалов, требующее согласия, которое с точки зрения самоопределения поставщиков данных, должно быть основано на балансе между нереалистично узкой областью действий и чрезмерно широком характере разрешения на использование данных. В данном случае динамические модели, в рамках которых неоднократно запрашивается согласие в отношении отдельных элементов использования данных, дополняются добавочными вариантами, такими как возможности делегирования. Участники также могут принять решение о том, какую форму согласия они в основном предпочитают.

(59) Чтобы оценить самоопределение, мы должны также учитывать социальный контекст, в котором находится участник. Чтобы быть свободным и иметь возможность действовать с помощью средств самоопределения, в этом свете должна иметься, по крайней мере, реальная возможность сохранения и формирования своей личности, принимая на себя ответственность за себя и других за свои действия. Это требует надежных и справедливых стандартов в соответствии с верховенством закона, которые одинаково применимы ко всем.

(60) Конфиденциальность классифицируется как право быть в одиночестве, или, другими словами, как область личного существования, когда в значительной степени исключается необходимость оправдывать себя или подчиняться нежелательному общественному контролю. Тесно связанное с конфиденциальностью или неприкосновенностью личной жизни понятие интимной жизни, которое определяет области жизни, предназначенные только для тех, кто непосредственно связан с ними, и какие-либо подробности предоставляются отдельным третьим лицам при наличии четкого согласия, если это вообще возможно.

(61) В значительной степени идеи о том, что считать частным или интимным, в культурном отношении переменны. Вообще говоря, сохранение частной сферы может быть нормативно оправдано на основе ее основного социального антропологического значения. Только в частной сфере можно закрыться от социальных отношений и сформировать условия для личного развития. Конфиденциальность создает пространство для близости и знакомства, в котором люди могут следить за отношениями и, без маскировки или торможения, действительно быть самими собой - защищены снаружи, но открытые внутри.

(62) Что касается большого объема данных, потенциальные угрозы конфиденциальности возникают из-за многочисленных новых возможностей, появляющихся для сбора, анализа и перекомпоновки данных и информации, а также сопутствующих проблем, связанных с обеспечением анонимности и псевдонимизации. Более интимные подробности могут быть представлены в цифровом виде, но при этом возрастает риск самопроизвольного внешнего контроля или информационной опасности для личного образа жизни, который оказывается в значительной зависимости от внешних воздействий.

(63) Даже если общий контроль над своим полным информационным отчетом невозможен в цифровом обществе, люди тем не менее считают важным, чтобы они могли определять, в зависимости от данных обстоятельств, как их данные используются и используются повторно. В то же самое время пользователи данных, как ожидается, будут обрабатывать данные, доступные для них, конфиденциальным и заслуживающим доверия способом, даже при анализе вне контекста и повторном сопоставлении возможностей и контекста этих данных.

(64) Вопрос о том, как защитить конфиденциальность в условиях большого объема данных, влияет не только на отдельных лиц, но и на группы. Анализ больших объемов данных часто демонстрирует сочетания характеристик, которыми пользуются многие люди. Те, кого это касается, сгруппированы по алгоритмам с потенциально позорящими, дискриминационными или ограниченными по характеру последствиями. Отдельные лица часто не знают о том, чтобы они разделяются по категориям таким образом.

(65) Решающее значение в контексте большого объема данных имеет понятие суверенитета. С его культурно-историческим происхождением, лежащим преимущественно в политико-религиозной сфере, понятие суверенитета принимает различные конкретные формы во многих областях жизни. Это понималось как собственность Бога или абсолютистского правителя, в силу которого человек, полностью и невзирая на другие силы, мог что-либо делать или допускать. Вместо этой якобы абсолютной свободы суверенного субъекта другие понимания суверенитета подчеркивают то, как физическое и социальное воплощение субъекта зависит от внешних факторов.

(66) Согласно пониманию суверенитета, который по крайней мере принципиально исключает понятие о том, что один человек может властво-

вать над другим, данные личного характера просто передаются специалистам по сбору информации и пользователям; эти данные не являются свободно и произвольно доступными. Однако, наоборот, это не означает, что поставщики данных автоматически являются владельцами своих данных, и это не означает, что они могут реализовать свои требования к суверенитету при любых обстоятельствах. Тем не менее, это понятие влечет за собой широкие возможности для контроля над личностью.

(67) Концепция суверенитета тесно связана с понятием власти. Суверенитет реализуется при осуществлении власти; наоборот, он ограничен другими лицами, осуществляющими свою собственную суверенную власть. В контексте большого объема данных конкретные способы осуществления власти имеют этическое значение: во-первых, такие способы, с помощью которых можно манипулировать предпочтениями и убеждениями других; и, во-вторых, такие, которые идут дальше, даже позволяя тонкое формирование, модификацию и, следовательно, потенциальное управление характерами других лиц.

(68) Использование алгоритмов с большими объемами данных позволяет предлагать онлайн-сервисы с новыми возможностями для оказания целенаправленного воздействия на мысли, чувства и действия своих пользователей. Спектр воздействий простирается от открытого подталкивания, благодаря которому поведение, благоприятное для здоровья, должно поощряться, до скрытых вмешательств в своих целях, которые, в значительной степени, предназначены для достижения выгод другим. Эти вмешательства, по крайней мере, нуждаются в неотложном этическом оправдании, поскольку они уклоняются от когнитивного контроля над теми, для кого они предназначены, обходя способности пострадавшего человека управлять характером его (или ее) действий, и тем самым, подрывая их самоопределение.

(69) Еще одна важная нормативная точка отсчета вытекает из морального обязательства о благотворительности, согласно которому действия кого-либо в многочисленных ситуациях следует взвешивать таким образом, чтобы они приводили не только к минимизации издержек, но и к выгоде других, особенно нуждающихся , Два аспекта понятия благотворительности представляют особый интерес в связи с темой большого объема данных и здоровья: расширение знаний и понимания, а также совершенствование лечения, в результате чего для различных вовлеченных сторон возникают новые возможности, открывающиеся при сборе цифровой информации и обработке больших объемов данных в секторе здравоохранения.

(70) Знание и понимание важны в самосознании личности и ее способности жить автономно. Кроме того, критический анализ, защита и расширение объема знаний выполняют важную социальную функцию.

(71) Обеспечение коммуникационной связи ради достоверности необходимо для достижения целей, связанных с продвижением знаний. В частности, в области науки разработаны сложные методологические и теоретические стандарты для обеспечения такой связи. Поэтому следует позаботиться о том, чтобы не позволить новым цифровым методам сбора, анализа и рекомбинации данных вызвать ослабление эпистемологических стандартов14 или к потере надежности доказательств, которые они генерируют.

---

14 Стандарты эпистемологии – философско-методологической дисциплины, исследующей знание как таковое, его структуру, функционирование и развитие. Она изучает отношение “субъект - знание”.

(72) Остаются также вопросы о том, какие группы должны в первую очередь извлекать выгоду из достижений в области знаний, которые могут быть получены от большого объема данных, о том, как можно преодолеть существующие препятствия для более эффективного планирования процесса использования данных и как может быть достигнуто справедливое распределение положительных эффектов в результате ожидаемых успехов в расширении знаний.

(73) Сбор и передача больших объемов данных, имеющих отношение к здоровью, затрагивает фундаментальные вопросы справедливости. В качестве нормализующего принципа социальных отношений в целях справедливости требуется избегать произвольных привилегий некоторых лиц или групп. Скорее, он должен быть определен на рациональной основе справедливым и пропорциональным для каждого человека способом. Это требует применения единых критериев, а различия в обращении с различными лицами должны быть нормативно обоснованы способом, позволяющим достичь социального консенсуса.

(74) Что касается приложений с большими объемами данных в секторе здравоохранения, то четыре проблемы имеют особое значение для вопросов справедливости: во-первых, доступ к наборам данных для исследовательского сектора; во-вторых, постепенно развивающаяся консолидация монополистических структур; в-третьих, включение приложений для здоровья, а также различных устройств, которые облегчают частный самоконтроль, при определении премий медицинского страхования; и, в-четвертых, аспекты социальной справедливости, понятные с точки зрения подхода к возможностям, поскольку они касаются ответственного рассмотрения данных, относящихся к здоровью.

(75) Концепция солидарности означает просоциальное поведение[15], практику и предрасположенность, а также институциональные, политические и договорные положения, целью которых является помощь другим. Солидарность часто понимается как дополняющая - и часто вспомогательная - концепция справедливости. Она регулярно возникает на фоне общих целей группы перед лицом общей проблемы или на основе общей идеи о хорошей жизни в рамках взаимодополняющего сообщества.

(76) Солидарность часто основывается на ожиданиях взаимности. Готовность действовать солидарно может уменьшиться, когда возникают сомнения относительно реалистичности таких ожиданий. Это может произойти, например, когда в конечном итоге создается впечатление, что потребность других в помощи и поддержке навязывается самим себе в результате их небрежного поведения и отсутствия инициативы, что приводит к перегружению структуры солидарности.

(77) Способность, предоставляемая большим объемом данных анализировать все более всеобъемлющие и разнообразные данные, относящиеся к здоровью, позволяет создавать более точные профили рисков. В связи с этим возникает озабоченность тем, что основное предположение о солидарности, на котором действует система обязательного медицинского страхования, а также справедливое структурирование контрактов в частном секторе медицинского страхования, - это то, что уязвимость к рискам для здоровья является чем-то общим для всех - может оказаться под вопросом.

[15] Просоциальное поведение – социальное поведение, которое приносит пользу другим людям или обществу в целом.

Это позволило бы группам с низким уровнем риска в большей степени отказаться от взаимодополняющей группы лиц, застрахованных на законных основаниях, значительно увеличив бремя тех, кто должен оставаться.

(78) В рамках системы обязательного медицинского страхования премии, установленные на основе поведенческих данных, подрывают понятие солидарности, которое требует защиты от уязвимости, связанной с болезнью, в значительной степени без учета рисков, связанных с индивидуальным поведением. С другой стороны, частное медицинское страхование работает с премиями за риск. Однако здесь перераспределение рисков в пользу держателей страховых полисов может привести к тому, что, даже после заключения договора страхования, будущие премии будут регулярно корректироваться на основе непрерывного сбора и анализа отдельных данных, сделанных на основе большого объема данных. Это полностью отрицает основной принцип страхового покрытия, при котором риски взаимно переносятся большой группой, а премии не могут быть индивидуально подобраны. Потенциал будет расти для небольших пулов держателей страховых полисов, когда случаи болезни или травмы быстрее приведут к увеличению премий.

(79) Кроме того, владельцы частных страховых полисов, не желающие или не способные участвовать в модели страхования на основе поведения, могут быть лишены финансовых стимулов; в долгосрочной перспективе это приведет к невыгодным премиям. Независимо от того, проводят ли они к здоровому образу жизни, эти страхователи будут наказаны за то, что они не предоставили страховщику доступ к своим личным данным, и поэтому будут поставлены в невыгодное положение просто для осуществления своего права на информационное самоопределение.

(80) По сути, свобода жить своей жизнью и развивать свою личность, согласно собственным планам, имеет приоритет над строгим и постоянным обязательством избегать всех рисков для здоровья. Хотя этот принцип не применяется при любых обстоятельствах, с его помощью трудно определить постоянный целенаправленный сбор данных о своем индивидуальном образе жизни или использование профилей рисков, которые основаны на большом объеме данных, охватывающих все сферы жизни, в качестве разумного ожидания ответственности, которую можно нести за собственное здоровье.

(81) Остается предметом обсуждения, могут ли законодательно уполномоченные медицинские страховщики учитывать личную ответственность владельцев страховых полисов и влиять на их поведение, связанное с их здоровьем. Структуры стимулирования, основанные на данных, могут перерасти в высокоинтенсивные и насильственные формы наблюдения. С другой стороны, сложное выявление факторов риска с использованием анализа большого объема данных, интеграция данных из всех областей жизни, в будущем может идентифицировать, что подавляющее большинство населения характеризуется смешанными профилями риска, охватывающими как благоприятные, так и отрицательные факторы, и физические, умственные, поведенческие или иного рода.

(82) В различных областях медицины применение технологий с большим объемом данных уже привело к разработке новых, просоциальных методов взаимной поддержки, таких как, например, образование небольших групп пациентов, которые имеют один и тот же опыт или риски редких заболеваний. Это позволяет им комбинировать свои данные и биологические образцы в коллективных объединениях, чтобы они были в распоряжении исследователей по их конкретным наборам симптомов.

(83) Другие достижения в области солидарности в настоящее время можно увидеть на онлайн-форумах, где пациенты могут вводить данные, обмениваться, обсуждать и использовать для собственного управления здоровьем как самостоятельно собранную информацию, так и клиническую информацию, и опыт. По мере ускорения разработки онлайновых сетевых инструментов для самопомощи для пациентов ожидается расширение такой практики.

(84) В качестве моральной категории ответственность может быть дифференцирована в зависимости от типов действий и решений, а также в соответствии с организацией институциональных структур. Ответственность может быть востребована и принята нравственно, юридически, политически и договорно как до, так и после принятия решения или действия. Различные соответствующие виды ответственности часто существуют в объективно взаимозависимых отношениях: можно ожидать, что ответственность за будущее будет от тех сторон, которые можно было бы привлечь к ответственности в случае фактического ущерба. Комплексное взаимодействие между отдельными лицами, учреждениями и технологиями, связанное с использованием больших объемов данных, приобретает особое значение в областях, имеющих отношение к состоянию здоровья и здравоохранению. Чего следует избегать, это непрозрачного распространения ответственности, что представляет опасность в любой ситуации, связанной с взаимодействием многочисленных участников и высокотехнических процессов.

(85) В частности, в эпоху больших объемов данных требуется определенная структура, позволяющая отдельным поставщикам данных взять на себя ответственность за свои данные. Эта структура должна быть технически и организационно эффективной, и простой в использовании. В особо чувствительной области состояния здоровья и здравоохранения, кроме того, имеется повышенная обязанность по уходу, которая относится, например, к исследователям или врачам.

(86) Ключевым моментом для того, чтобы инженеры могли нести ответственность в свои процессы обработки большого объема данных, является необходимость создания фундаментальных условий для ответственного управления данными, предоставления уже аннулированного согласия и создания легкодоступных вариантов администрирования данных. Можно исключить из этих требований достаточно агрегированные данные, полученные данные или случаи, которые явно исключают идентификацию лиц из данных. Использовать такие подходы для облегчения процессов деконтекстуализации и реконтекстуализации, специфичных для больших данных, одновременно обеспечивая высокие стандарты анонимности и создавая доверие к учреждениям, использующим большие данные, является ключевой задачей, которую предстоит решить.

(87) Еще один способ для отрасли взять на себя ответственность за права человека, а также защищать законные интересы бизнеса - это использовать интерфейсы прикладного программирования для создания систем делегирования. Такие интерфейсы могут действовать как “система управления данными” при реализации предпочтений поставщиков данных относительно обработки их данных. Таким образом, индивидуальное управление данными будет заменено программной системой управления данными, предоставляющей отдельным лицам надежные и технически доступные средства для принятия на себя ответственности за выбор краткосрочных, среднесрочных и долгосрочных стратегий обработки своих данных, одновременно устраняя необходимость для принятия отдельного решения по каждому вопросу использования данных.

(88) Предприятия могут также взять на себя ответственность за счет усиления надзора и подтверждения их процессов с точки зрения, например, используемых алгоритмов; меры, принятые для ликвидации систематической дискриминации; соблюдение правил, касающихся хранения данных, анонимности и удаления; и беспроблемную и несанкционированную защиту происхождения, обработки, использования и обмена данными.

(89) Помимо правительственного регулирования существуют другие способы обеспечения и/или содействия принятию на себя ответственности со стороны институциональных субъектов. Сертификация, печать качества или добровольные стандарты, установленные и контролируемые заинтересованными или промышленными группами, могут, например, укреплять доверие к соответствующим организациям и процессам.

(90) Еще один вопрос об ответственности касается организаций, которые потенциально могут посягать на личное общение между пользователями, давая, например, советы и предложения, пропагандирующие здоровый образ жизни. С одной стороны, возражение против явных вторжений в частную или интимную сферу было бы против таких действий. С другой стороны, если бы функциональная надежность базовых алгоритмов была научно обоснована, то с этической точки зрения можно было бы учесть возможность того, что такие действия могут предотвратить серьезные страдания или даже смерть, как, например, в предложениях помощи в социальных сетях, предназначенных для лиц, подверженных риску самоубийства.

(91) Государство может взять на себя ответственность на национальном уровне, как часть ЕС, или как сторона международного права. Однако в связи с вышеупомянутыми трудностями, связанными с правовым применением, должен преобладать принцип нормативно-правовой субсидиарности[16], в соответствии с которым добровольные обязательства и сертификация имеют приоритет над подробными правовыми нормами, при условии, что первые являются эффективными.

(92) Что касается трех уровней потенциального распределения ответственности в области приложений с большим объемом данных, важных для здоровья (физических лиц, организаций и государства), то люди действительно обязаны взять на себя ответственность за использование своих данных. Тем не менее, в первую очередь, эти организации собирают, обрабатывают и передают эти данные, чтобы обеспечить условия для ответственного формирования информационной свободы со стороны поставщика данных.

(93) Чем меньше организаций желают или могут предоставить технические средства, с помощью которых отдельные лица могут легче контролировать свои данные, тем более актуальной становится потребность государства, с точки зрения этики ответственности, вмешиваться, чтобы гарантировать, надзор и, где это применимо, регулировать и санкционировать. Цель предоставления индивидууму способности суверенных отношений с их данными достижима только тогда, когда требуемая ответственность будет приниматься со всех сторон.

---

[16] Субсидиарность – принцип социальной организации, возникший в Римско-католической церкви. В соответствии с этим принципом социальные проблемы должны решаться на самом низком, малом или удаленном от центра, на котором их решение возможно и эффективно, а центральная власть должна играть "субсидиарную" (вспомогательную) роль.

Суверенитет данных как формирование информационной свободы

(94) Суверенитет данных, понимаемый как ответственное формирование информационной свободы, в соответствии с рисками и возможностями, представленными большим объемом данных, является центральной этической и правовой целью в решении проблем и возможностей, представленных большим объемом данных.

(95) Понятие формирования информационной свободы основывается на концепции информационного самоопределения. Оно не основан на исключительных правах, аналогичных собственности, а скорее на полномочиях каждого человека определять, с каким контентом выбирается отношение к более широкому миру. Формирование информационной свободы в этом смысле относится к интерактивному развитию личности в сетевом мире и характеризуется способностью эффективно вмешиваться в постоянный поток отдельных важных данных на основе личных предпочтений. Формирование такой свободы является важным, когда также ориентируется на юридические и социальные требования солидарности и справедливости.

(96) В соответствии с концепцией суверенитета данных, описанной здесь, мы не стремимся ни увековечить установленный, слегка модифицированный подход к регулированию защиты данных, не призываем к полной переориентации, не говоря уже об отказе от обычного понятия защиты данных или общего снижения существующего уровня защиты. Скорее, цель состоит в том, чтобы выполнить и обеспечить эффективные основные нормативные требования, описанные выше, в том числе касающиеся информационной самоопределенности, основанной на правилах этики и учитывающей точки зрения основных прав и, следовательно, относящихся к защите данных, в новых условиях больших объёмов данных.

(97) Защита данных не является и никогда не была самоцелью. Скорее, она служит для защиты человека - как частной сферы, так и свободного развития личности в общественной сфере. Однако с концепцией суверенитета данных мы также хотели бы подчеркнуть цель объединения суверенитета человека, т.е. самоопределения и ответственности, обработки своих личных данных с реализацией потенциала, открытого большими объемами данных, как для общества, так и для направления индивидуальных жизней.

(98) В качестве цели ответственное формирование информационной свободы в области состояния здоровья и здравоохранения заключается в том, чтобы в полной мере использовать потенциал, открытый большими объемами данных для медицинских исследований, клинической практики и индивидуального здоровья и связанного с здоровьем поведения, при одновременном снижении сопутствующие рисков до минимума.

(99) Что касается формирования и осуществления суверенитета данных, можно выделить две все более близкие и, по существу, перекрывающиеся сферы: во-первых, использование данных в медицинских исследованиях и клинической практике, которые до сих пор характеризовались относительно четкой и строгой защитой данных, качества и стандартов безопасности; во-вторых, есть чрезвычайно разнородные продукты и услуги на свободном рынке, которые все больше влияют на развитие в секторе здравоохранения. Последняя категория простирается от концепций приложений, которые граничат с первой сферой и ее стандартами с явно сомнительными продуктами, не включенными в устойчивое продвижение здоровья.

(100) Разработки в области больших объемов данных не могут быть остановлены, но ими, безусловно, можно управлять. Поскольку для этого не-

достаточно механизмов и форм действий, которые характеризуют традиционный закон защиты данных, задача заключается в разработке моделей для регулирования и формирования этих событий, которые более точно отражают их сложный и динамичный характер. Они должны отражать принцип суверенитета данных как формирование информационной свободы в многомерном виде и с учетом различных групп участников и контекстов действий, принимая во внимание возможные формы и определение ответственности, описанные выше.

(101) В условиях больших объемов данных необходимо отказаться от устаревших представлений о конкретном виде данных, имеющих определенную чувствительность, которая вызывает соответствующие защитные механизмы. Защита данных больше не может быть привязана к определенным категориям данных и использованию данных; скорее, она должна адаптироваться к постоянной перегруппировке и повторной контекстуализации данных.

(102) Модель, предназначенная для регулирования и формирования использования данных, ориентированная на принцип суверенитета данных, фокусируется на тех лицах, которые предоставляют данные как основные действующие лица, которых необходимо защищать и уважать. Цель состоит в том, чтобы дать возможность этим субъектам, а также организациям, связанным с ними, обеспечить суверенное регулирование своих данных, путем разработки правил и формирования институтов в соответствии с условиями, соответствующими каждому случаю. Упрощенных массовых решений следует избегать в пользу более сложных, институционально диверсифицированных, сложных моделей, которые являются гибкими и отвечают поставленным проблемам.

(103) Разнообразная вторая сфера, описанная выше, должна быть сформирована в соответствии со следующим основным принципом: чем ближе индивидуальное применение граничит с первой сферой, тем сильнее этический и юридический императив, чтобы управлять своим развитием со ссылкой на нескольких действующих лиц в сторону стандартов качества, защиты и доверия, которые обычно относятся к первой сфере.

Рекомендации

Германский совет по этике рекомендует концепцию управления, ориентированную на достижение центральной цели суверенитета данных. Такая концепция требует комплексных социальных усилий, включая как юридические, так и неюридические элементы, и включение технических достижений, доступных всем субъектам общества таким образом, чтобы гарантировать сохранение основных прав. Представленная здесь концепция управления содержит конкретные рекомендации для действий в четырех областях. Они направлены, во-первых, на реализацию потенциала больших объемов данных; во-вторых, обеспечить индивидуальную свободу и неприкосновенность частной жизни; в-третьих, обеспечить справедливость и солидарность; и, в-четвертых, содействовать ответственности и доверию. Рекомендуемые меры должны финансироваться и осуществляться как можно скорее.

A. Реализация потенциала

Чтобы реализовать потенциальные преимущества больших объемов данных в секторе здравоохранения, сотрудничество между многочисленными участниками клинической практики, основными медицинскими исследованиями и компаниями, занимающимися вопросами здравоохранения, а

также отдельными поставщиками данных должно быть максимально плавным. Цель должна заключаться не только в предполагаемом сборе и устойчивом доступе к наборам данных, но и в содействии сочетанию уже существующих наборов данных из клиники и исследований с вновь полученными данными с соблюдением этических норм.

A1. Создание необходимой базовой инфраструктуры

Возможность использовать потенциал больших объемов данных в секторе здравоохранения жизненно зависит от наличия высокопроизводительной инфраструктуры для сбора, хранения, анализа и передачи больших объемов данных. Чтобы избежать проблемных зависимостей от коммерческих поставщиков для этих инфраструктурных служб, которые часто не подпадают под стандарты немецкой или европейской защиты данных, государственные органы должны обеспечить, чтобы такая инфраструктура, особенно для клинической практики и основных медицинских исследований, строилась и развивалась быстро, чтобы обеспечивался адекватный доступ, и чтобы он подлежал общественному контролю.

A2. Содействие обмену данными и интеграции

Также важно, чтобы ответственный обмен и учет данных, относящихся к здоровью, между несколькими институциональными субъектами обеспечивался рядом мер и достаточным государственным финансированием для их осуществления:

A2.1. Разработка и внедрение стандартных процедур совместимости данных

Чтобы обеспечить адекватное группирование данных из разных источников, при соблюдении права поставщиков данных на неприкосновенность частной жизни данные должны быть сопоставимы с другими данными; т.е. они должны быть последовательно помечены и соответствующим образом аннотированы. Решающее значение для этого требует стандартизация форматов данных и создание вариантов контроля качества, включая прозрачную документацию о предпринятых шагах.

A2.2. Уточнение совместного управления данными исследований

Нынешние инициативы по созданию структур для эффективной коммуникации, сотрудничества и координации между участвующими учреждениями должны быть объединены, усилены с учетом долгосрочной перспективы. В то же время необходимо уделять внимание обеспечению надлежащего взаимодействия с инфраструктурой телеинформатики, а также согласованию с дальнейшим развитием обмена данными в секторе здравоохранения, как указано в E-Health-Gesetz (Закон об электронном здравоохранении).

A3. Содействие и защита качества данных и исследований

Первоочередной задачей является обеспечение качества данных для получения достаточно надежных результатов. Для этого необходимы следующие меры:

A3.1. Соблюдение эпистемологических стандартов, особенно доказательной медицины

Поскольку механизмы контроля безопасности и эффективности медицинских вмешательств развиваются так, что они могут заниматься приложениями с большими объемами данных, не следует подрывать установленные стандарты доказательной медицины. При обслуживании медицинских приложений процессы, основанные на больших объемах данных, также должны быть подвергнуты установленным клиническим испытаниям на предмет безопасности и эффективности.

A3.2. Внедрение единых стандартов данных и документации

Внедрение единых стандартов представляет собой разумную меру не только в плане обеспечения взаимодействия и сотрудничества, но и для обеспечения эффективного контроля качества. Например, это включает вопросы, касающиеся форматов данных и метаданных, поэтапную реконструкцию процесса использования данных, управление версиями и сопоставление семантических ссылок и иерархий данных самым последовательным образом. В частности, стандарты качества для данных должны включать требования к документации, чтобы облегчить отслеживание происхождения данных и, по крайней мере, их будущую прослеживаемость.

A3.3. Создание печатей качества данных

Чтобы обеспечить прозрачность вышеупомянутых стандартов качества и их основополагающих требований, должны быть присуждены сертификаты соответствия ("печать качества"), которые достоверно демонстрируют происхождение и качество исходных данных и шаги обработки, которые они претерпели (например, с помощью технологии блокировки). Поскольку обеспечение качества также отвечает интересам различных действующих лиц, основное внимание следует уделять механизмам внутреннего мониторинга в науке и промышленности. Тем не менее, поскольку они оказываются недостаточными, следует также ввести всеобъемлющие правовые требования.

A4. Адаптация правовой основы для использования данных в исследовательских целях

A4.1. Дальнейшее развитие вторичного использования исследовательских данных

Там, где это применимо, закон защиты данных позволяет на основе тщательного взвешивания интересов обрабатывать персональные данные даже без согласия - если данные служат и необходимы для научных, исторических или статистических целей (статья 27 Федерального закона о защите данных, новая версия) - тогда в принципе необходимо использовать дополнительные процедурные меры защиты и проектирования, такие как модели каскадного согласия (см. Рекомендацию B2), в интересах суверенитета данных.

A4.2. Содействие юридическим возможностям человека, позволяющим в полной мере использовать их данные для целей медицинских исследований ("дарение данных")

В принципе, традиционная модель согласия требует, чтобы личные данные собирались только в строгих пределах, предписывающих их предполагаемое использование. Именно потому, что должна соблюдаться модель согласия, необходимо не только расширять ее процедуры, но и становиться более открытыми для конкретных областей. В частности, это должно облегчить способность человека разрешать с помощью соглашения о всеобъемлющем согласии использование своих данных без строгого целевого назначения для целей фундаментальных клинических и медицинских исследований ("дарение данных"). Предпосылкой было бы полное разъяснение возможных последствий, особенно в отношении прав других лиц, таких как затронутые члены семьи. Также необходимо было бы научно обоснованное развитие соответствующей инфраструктуры для сбора, хранения, наблюдения, обработки и передачи таких предоставленных данных.

A5. Содействовать внедрению цифровых систем поддержки принятия решений в клинической практике

Следует ускорить как поощрение взаимного обмена знаниями между исследовательской и клинической практикой, так и утверждение цифровых услуг для поддержки решений, которые могут улучшить уход за пациентами. С этой целью при сохранении суверенитета данных необходимо предоставить легитимированным субъектам максимально широкий доступ как к данным, получаемым в результате исследований, так и к предоставлению медицинских услуг, а также к соответствующим приложениям для крупных данных, относящимся к здоровью.

A6. Продвижение международной коммуникабельности

В целях международного обмена данными усилия по стандартизации не должны ограничиваться национальными территориями. Скорее, необходимо приложить далеко идущие усилия на всех уровнях (политика, наука и технологии) для согласования стандартов.

В целях повышения международной конкурентоспособности немецких и европейских цифровых приложений в секторе здравоохранения, включая высокие стандарты защиты качества и данных, которые требуются в этом секторе, а также для борьбы с проблемными зависимостями в этом секторе, инвестиции в медицинскую информатику должны быть гораздо шире и делаться быстрее, чем планировалось ранее. В частности, целенаправленное совершенствование управления данными в государственных больницах представляется в высшей степени разумным.

B. Обеспечение личной свободы и конфиденциальности

Готовность передавать свои личные данные в распоряжение третьих сторон должна пониматься как часть информационной свободы как поставщика данных. Поставщики данных, таким образом, должны иметь возможность обрабатывать свои данные независимым образом и сознательно формировать свои частные сферы. Кроме того, необходимо создать структуру, которая гарантирует надлежащий объем действий.

B1. Обеспечение суверенитета поставщиков данных по их личным данным

В свете способности большого объема данных перекомпоновывать данные и отделять их от конкретных целей, способность определения, осуществляемая поставщиком данных по их личным данным, должна быть гарантирована в максимально полной степени.

B1.1. Открытые программные интерфейсы для поставщиков данных ("информационные агенты")

Особенно в ситуациях, когда объем использования данных не может быть точно разграничен заранее или, когда сбор данных и их обработка непрерывны, соответствующие программные инструменты ("информационные агенты") должны быть доступны в качестве дополнения к обычно используемым моделям согласия. Они будут управлять подачей данных в соответствии с ожиданиями поставщика данных, что позволит повысить контроль, прозрачность и отслеживаемость. Соответствующие программные интерфейсы должны быть стандартизированы с помощью саморегулируемых или законодательных средств для облегчения разработки таких информационных агентов. Правильное функционирование интерфейсов и информационных агентов должно поддерживаться мерами аудита или сертификации.

B1.2. Содействие совместному определению поставщиками данных распространения данных

При распространении данных необходимо обеспечить обратимость сбора данных: любая система, которая собирает персональные данные и принимает ее вход, должна - за исключением обоснованных исключений - иметь возможность полностью или частично удалить эти данные. Здесь также должна быть развернута модель информационных агентов, интегрированных как мониторы в конвейеры данных. Через подходящие каналы связи (например, соответствующее приложение) поставщика данных следует попросить дать согласие на распространение своих данных и, в зависимости от случая, иметь возможность ограничить или отменить его с относительной легкостью.

B1.3. Уточнение юридических проблем, связанных с предполагаемым владением данными

Суверенитет данных не следует путать с "владением" данными. Поскольку концепция собственности подразумевает ее основные правовые элементы - постоянные, фиксированные отношения и абсолютную силу исключения по отношению к третьим сторонам – она плохо подходит для задачи обеспечения суверенитета данных. С другой стороны, поскольку необходимо признать определенный (хотя и гибкий) личный суверенитет над данными со стороны индивида, имеет смысл сосредоточиться вместо этого на правовой основе для использования данных. Германский совет по этике рекомендует учредить всеобъемлющую экспертную комиссию по этому вопросу, которая будет оснащена не только юридической экспертизой, но и междисциплинарным подходом.

B2. Создание каскадных моделей согласия

В принципе, в клинической практике и медицинских исследованиях (модель выбора) следует продолжать применять концепцию нормативного регулирования на основе согласия. Кроме того, по возможности следует использовать каскадные модели согласия, предлагать разнообразные, динамичные способы предоставления или делегирования согласия (например, независимому доверенному лицу/учреждению или аналогичному субъекту) - один раз, регулярно или для каждого индивидуального решения. При условии, что базовая позиция уважения к частной сфере наряду с гарантиями и стандартами качества, разработанными в этом мнении, гарантирована, модели, которые доказали свою эффективность, особенно в области хранилища биологических материалов, должны передаваться и адаптироваться к другим секторам.

B3. Обеспечение конфиденциальности по умолчанию

Из-за нехватки времени или понимания, субъективно воспринимаемого отсутствия альтернатив или добросовестно, поставщики данных часто просто принимают настройки по умолчанию для приложений сбора данных и обработки данных. Поэтому стандартные настройки должны быть технически разработаны с соблюдением правовых гарантий для обеспечения надлежащей защиты конфиденциальности с самого начала (конфиденциальность по дизайну/ конфиденциальности по умолчанию). Это относится, в частности, к пока еще относительно нерегулируемой области приложений частного сектора, таких как приложения, связанные со здоровьем для мобильных устройств и связанные с ними датчики и устройства наблюдения. В дополнение к положениям GDPR относительно пользовательских настроек необходимо предоставить дополнительную информацию, чтобы пользователи действительно понимали последствия изменений основных настроек.

B4. Разъяснение и обеспечение прозрачности использования алгоритмов

Помимо существующих требований юридической информации цели, функции и механизмы сбора данных и любые используемые алгоритмы должны быть понятными для неспециалистов. Принимая во внимание необходимость защиты интеллектуальной собственности, эта информация должна включать, в частности, следующее:

>> какие данные пользователя вводятся в какие анализы, модели прогнозирования и принятие решений или процессов отбора, и какие показатели не собираются в явной форме и не вводятся для того чтобы, например, избежать дискриминации,

>> какие выводы, выводы, прогнозы, выбор или решения получены и сделаны с помощью алгоритмов, работающих с этими данными,

>> каким образом создаются профессиональное досье поставщиков данных и какая ожидаемая надежность может быть обеспечена такими полученными переменными,

>> в какой форме анонимные личные данные поступают в (статистические) модели и у кого есть права на их использование.

B5. Противодействие обману и манипуляциям

Необходимо проводить различие между открытыми, прозрачными способами воздействия на других и более проблематичными формами скрытого вмешательства, которые целенаправленно обходят когнитивный контроль[17] над теми, кого это касается. Связанное с манипуляциями приобретение и использование данных, которое обманывает поставщика данных в отношении, например, характера и цели сбора данных, и/или использует их неспособность понять его последствия, является юридически и морально неприемлемым. Особенно в социальных сетях, приложениях и онлайн-играх, как правительственные органы, так и сами операторы должны работать более энергично, чтобы противодействовать таким тенденциям.

B6. Содействие цифровому образованию

Предпосылкой суверенитета данных является базовое понимание значимости и ценности большого объема данных, а также связанных с ними рисков. Учитывая, что дети также используют цифровые приложения и генерируют данные, необходимая компетентность пользователей уже должна быть получена в школе. Помимо чисто технических аспектов обычных стратегий для цифрового обучения класса, придание этой компетенции следует рассматривать и воспринимать как задачу, которая касается всех предметов. Это будет противодействовать информационной опасности, которая в настоящее время является эндемичной среди детей и подростков, и позволит своевременно выявлять соответствующие юридические, социальные и этические последствия. Возможность передать необходимую компетентность пользователю должна как таковая быть неотъемлемой частью будущей подготовки учителей. Кроме того, учреждения, обучающие взрослое население, должны постоянно готовить доступные для понимания предложения для всех возрастов в этой области, тогда как компании и учреждения должны проводить регулярную внутреннюю учебную подготовку.

B7. Повышение уровня дискуссии и участия

Необходимо более активно развивать текущие публичные дебаты по большому объему данным. С этой целью государство должно работать над предоставлением надежной информации и установлением процессов участия. Это должно гарантировать широкое участие общественности и открытый обмен со специалистами и профессионалами.

C. Обеспечение справедливости и солидарности

C1. Создание справедливого доступа к цифровым услугам

Некоторые группы пользователей регулярно исключаются из преимуществ перевода информации в цифровую форму в результате, например, образовательных барьеров. Для противодействия таким факторам необходимы не только специальные информационные и образовательные поло-

[17] Комплекс исполнительных функций, позволяющих индивиду регулировать поведение согласно текущим задачам.

жения; следует также принять меры к тому, чтобы цифровые услуги не были с самого начала спланированы таким образом, чтобы быть эксклюзивным. Это может быть результатом непонятных или излишне сложных средств работы или излишне технического языка. Программное обеспечение и пользовательские интерфейсы должны быть сконструированы таким образом, чтобы они были максимально беспрепятственными.

C2. Раскрытие и предотвращение дискриминации и маргинализации

Необходимо принять меры для обеспечения того, чтобы расширенный объем информации, предоставляемой большими данными, на основе которых можно принимать решения о распределении средств, связанных с здравоохранением, не подвергается неправильному обращению, таким образом, что определенные лица или группы людей подвергаются дискриминации или маргинализации. При применении скрытых закономерностей, выведенных при анализе большого объема данных, существует острая опасность того, что базовые данные, выбранные параметры анализа и/или используемые алгоритмы могут привести к результатам, которые повлекут за собой систематические и развивающиеся постепенно формы дискриминации людей или групп людей. По этой причине необходимо не только заранее предусмотреть недопустимость определенных, соответствующих критериев отбора, если они не имеют четкой и надлежащей цели, а также разработать процедуры, позволяющие выявлять и санкционировать возможные нарушения. Даже если вспомогательное саморегулирование по секторам или самим учреждениям является эффективным в этом отношении, оно должно дополняться принудительно установленными правительством санкционированными и судебными гарантиями.

C3. Допущение возражения на автоматизировано принятые решения

При рассмотрении решений, которые принимаются на основе алгоритмов, необходимы структурные формы возражения и корректировки. В частности, в области частного страхования должно быть гарантировано право страхователя на четкое, понятное и индивидуальное обоснование отклоненного требования о компенсации, а также свободный и низкий уровень доступа к внутренним и внешним апелляционным и арбитражным органам.

C4. Защита уязвимых лиц и групп

Особое внимание должно быть уделено отдельным лицам и группам, которые из-за индивидуальных или социальных обстоятельств могут (по крайней мере временно) более подвержены прямому или косвенному, структурному или намеренному отказу в выгодах или непропорционально нести расходы на цифровые услуги в секторе здравоохранения. Это особенно касается детей и молодежи, а также пожилых людей и людей с ограниченными возможностями. Мало того, что эти лица должны поддерживаться с точки зрения развития их способности использовать цифровые услуги ответственно, им также необходимо, в силу своей особой уязвимости, получить особую защиту в процессе сбора и использования данных. В этом отношении суверенитет данных также учитывает индивидуально и ситуационно изменяющуюся способность ответственности со стороны тех, кого затрагивают большие данные.

C4.1. Строгое соблюдение требования согласия для детей и подростков

Положения GDPR в отношении согласия несовершеннолетних в отношении услуг информационного общества должны быть быстро и подобающим образом реализованы. Решения относительно варианта снижения минимального возраста согласия (допускаемого по GDPR) не должны приниматься без участия заинтересованных лиц (т. е. детей и подростков).

C4.2. Разработка механизмов защиты данных для других с ограниченной способностью к согласию

Необходимо разработать специальные механизмы защиты данных, чтобы регулировать сбор данных от других лиц, которые имеют ограниченную способность давать согласие, но не препятствуют потенциальному проведению исследований на основе больших объемов данных и в интересах таких лиц. Участвующие исследовательские учреждения должны обеспечить, чтобы информация, достаточная для принятия обоснованных решений, предоставлялась как пострадавшим лицам в соответствии с их когнитивными способностями, так и лицами, обеспечивающими уход за ними, в соответствии с принципом принятия решений.

C4.3. Ограничительное регулирование использования чатботов[18]

Использование чатботов для сбора данных от лиц, имеющих ограниченные когнитивные способности, или имеющих отношение к ним, влечет за собой особенно высокий потенциал для манипуляций, и поэтому его следует регулировать чрезвычайно ограничительным образом.

C5. Меры защиты медицины, ориентированной на уход

Личное внимание и забота о пациенте в медицинской практике должны быть усилены, а не скомпрометированы с помощью применения больших данных. Время и деньги, сэкономленные путем увольнения персонала, выполняющего рутинные работы или обеспечивающие более быструю и точную диагностику с помощью цифровых алгоритмов, должны приводить к повышенному личному вниманию пациентов.

C6. Обеспечить эффективную ответственность компаний, работающих с данными в секторе здравоохранения

Учитывая риски, связанные с большими данными, представляется целесообразным разработать специально разработанные модели ответственности. Здесь необходимо в первую очередь установить, достаточны ли и в какой степени новые правила, содержащиеся в немецком законе о защите данных (который пока не исчерпывает возможности GDPR). В рамках GDPR предусматривается введение строгой ответственности для обеспечения личности эффективной защиты от убытков. Принимая во внимание неопределенность ответственности и нормы доказательного права, следует рассматривать такую форму строгой ответственности, учитывающую кон-

[18] Чатбот – система искусственного интеллекта – виртуальный собеседник.

кретные риски больших объемов данных. Независимо от разрешения применения, это обязательство должно быть исключено, только в том случае, если ущерб неизбежен. Сумма любого потенциального ограничения ответственности должна быть установлена достаточно высокой, чтобы оказать заметное влияние на крупные компании.

D. Содействие ответственности и доверию

D1. Гарантийная защита и стандарты качества

D.1.1. Установление наилучших возможных стандартов защиты от несанкционированной идентификации лиц из анонимных, искусственно анонимных или обобщенных наборов данных

Учитывая неадекватную защиту, предлагаемую методами анонимности и искусственной анонимности, необходимо создать адекватные дополнительные гарантии для смягчения риска повторной идентификации:

>> Если идентификаторы (например, электронная почта, логин, идентификационный номер устройства, идентификатор файла cookie[19]) допускают относительно прямые выводы относительно затронутых лиц, они должны быть заменены анонимными ключами, срок действия которых должен истекать как можно быстрее.

>> Когда анонимный пользователь прямо или косвенно обнаруживает свою личность, либо неожиданно, либо случайно (например, случайное раскрытие своего имени, электронной почты, номеров телефонов, номера кредитной карты, идентификационного номера и т. д.), сборщик данных должен обеспечить, чтобы эта идентификация была отменена путем удаления данных.

>> В тех случаях, когда набор данных с помощью сочетания определяющих признаков и данных позволяет идентифицировать пользователя с высокой степенью вероятности, эти данные должны подчиняться тем же правилам защиты данных, что и явные идентификаторы.

>> Если соединения между наборами данных приводят к определенному снижению уровня защиты, эти наборы данных должны быть локализованы или подключены только кратко (т. е. без постоянного хранения в базе данных) и для четко определенных целей.

D.1.2. Компенсация пробелов в анонимности путем контроля доступа к данным

Учитывая постоянный риск повторной идентификации, контроль доступа к данным имеет особое значение. В частности, в клинической практике и основных медицинских исследованиях доступ к данным должен быть надлежащим образом ограничен уполномоченными сторонами. Это должно быть выполнено путем хранения данных в защищенных, технически изолированных и независимых хранилищах и создания контролируемых средств доступа, включая надежные системы проверки и аутентификации.

[19] Небольшой фрагмент данных, отправленный веб-сервером и хранимый на компьютере пользователя.

D.1.3. Обеспечение и подтверждение выполнения требований защиты

Суверенитет данных требует сосуществования технических и нормативных стандартов. В дополнение к существующим принципам обеспечения конфиденциальности по каждому лицу, которое занимается обработкой и использованием данных, следует стремиться обеспечить, чтобы соображения конфиденциальности были приоритетом для любого проекта, использующего большие объемы данных, начиная с этапа планирования и разработки. Эта обязанность должна также возлагаться на соответствующие учреждения (в исследованиях, в медицинской практике или в коммерческой области), чтобы продемонстрировать соблюдение правил, направленных на обеспечение суверенитета данных в их соответствующих областях ответственности. В дополнение к существующему опыту сотрудники по внутренней защите данных должны в дальнейшем развивать свои сферы ответственности и полномочия в этом направлении (управление корпоративными данными).

D1.4. Установление требований к отчетности о неудачах и неумелом выполнении своих обязанностей

Необходимо следить за тем, чтобы любые ошибки и неправильное поведение при обработке данных не скрывались, но вместо этого имелось понимание с точки зрения их значимости для всей системы, и чтобы они были тщательно изучены. Это повлечет за собой обязанность информировать потенциально пострадавших пользователей и, в той мере, в которой они не могут быть идентифицированы, общественности, а также сообщать о нарушениях надзорным организациям/органам.

D2. Совершенствование механизмов контроля

D2.1. Усиление роли сотрудников по защите данных

Для обеспечения суверенитета данных требуется определенное количество внутренних (частных) и внешних (государственных) надзорных органов, чьи обязанности должны быть лучше разграничены, и чей потенциал и экспертные знания должны быть расширены, когда это необходимо. В частности, крайне важно и необходимо переориентировать роль существующих сотрудников по защите данных - как в государственном, так и в частном секторах - в целях обеспечения суверенитета данных и, при необходимости, для расширения их обязанностей. Они должны дополнять работу местных надзорных органов, таких как комитеты по этике исследований, и должны смягчать и разрешать на основе прозрачных критериев принятие решений в конфликтных ситуациях. Поскольку существующие структуры контроля оказываются недостаточными для решения конкретных проблем, возникающих в результате наличия больших объемов данных, например, в межрегиональных и международных совместных проектах, следует учитывать большую централизацию.

D2.2. Назначение аудиторов данных

В свете того, что качество данных важно для общества в целом, особенно в медицинских исследованиях и клинической практике, должна быть создана соответствующая структура обзора и контроля. Это не обязательно

должно включать исключительно государственный орган; он также может функционировать как частное регламентирование, аналогичное, например, финансовому аудиту и бухгалтерскому учету в корпоративном праве.

D2.3. Внедрение моделей охраны данных

Чтобы способствовать доверию и предотвращению злоупотреблений, те, кто использует данные, должны закладывать техническую и организационную основу для обеспечения того, чтобы данные о запасах не обязательно предоставлялись им непосредственно, но могут быть введены модели охраны (например, благотворительные фонды). Это может не только смягчить дисбаланс власти; он также может противодействовать конфликту интересов. По крайней мере, в области медицинских исследований и клинической практики необходимо принять меры для обеспечения эффективности таких моделей, особенно в отношении пользователей данных, работающих в международном контексте (например, Google, Apple, Facebook, Amazon и Microsoft).

D3. Разработка кодексов поведения для исследований, клиник и промышленности

Используя существующие кодексы поведения в качестве модели, следует предпринять последовательные и постоянные усилия для установления всеобъемлющих внутренних стандартов поведения во всех областях, чувствительных к вопросам защиты данных. Это должно включать не только учет применимых нормативных требований и их укрепление в случае необходимости, но также, по крайней мере, в промышленности или в связи с конкретными областями применения, для обеспечения координации и согласования между национальными границами.

D4. Поддержка и расширение печатей качества для поставщиков услуг и приложений

Поскольку обеспечение соблюдения принципа суверенитета данных отвечает интересам пользователей данных, следует поддерживать и расширять систему классификаций на рыночной основе (печатей качества), некоторые из которых уже существуют. Таким образом, усилия по достижению минимальных стандартов и соблюдению обязательных правовых требований могут помочь структурировать компанию по отношению к конкуренции. Поскольку эти механизмы саморегулирования оказались неадекватными, должны быть введены меры совместного регулирования, например, в форме официальных сертификатов. Необходимо также укреплять структуры государственного контроля, включая положения об ответственности.

D5. Укрепление компетентности в ответственном обращении с данными среди всех, кто профессионально связан с большими объемами данных

В областях, где роль больших объемов данных быстро расширяется, необходимо повысить осведомленность об этических проблемах и новых обязанностях, связанных с использованием данных, относящихся к здоровью. Для осуществления таких культурных изменений необходимо улучшить по-

нимание исследовательской и информационной этики всех вовлеченных сторон, а также способность научно и критически отражать свои собственные действия. Наделение этими областями ответственности должно стать обязательным элементом профессиональной подготовки, а также высшего и дальнейшего образования, затрагивающего все соответствующие темы и области. Чтобы обосновать сложность и значение этого вопроса, например, компании и учреждения могли бы расширить свои усилия по созданию отделов внутренних данных.

>> Голосование “против”

В своем голосовании “против” Кристиан Фишер[20] (Christiane Fischer) призывает отказаться от использования большого объема данных для исследовательских целей или других приложений, если не гарантируется полная защита данных, внедрение эффективных анонимных и псевдоанонимных стандартов и право на забвение.

[20] Магистр технических наук, доктор технических наук, Дунайский институт непрерывного образования в Кремсе, Австрия, факультет здравоохранения, Центр медико-санитарных дисциплин.