2023; 4: 108-117 США & Канада: экономика, политика, культура / USA & Canada: economics, politics, culture

УДК: 341.1/8
DOI: 10.31857/S2686673023040089
EDN: VGRGGY

Сравнительно-правовой анализ вопросов защиты персональных данных в процессе развития искусственного интеллекта

М.Э. Гулиева

Финансовый университет при Правительстве Российской Федерации.
Российская Федерация, 125167, Москва, Ленинградский проспект, д. 49/2.
Researcher ID: HPD-5668-2023 *Scopus Author ID:* 57224857847 *РИНЦ ID: 1012999*
ORCID: 0000-0002-3961-0135 e-mail: MEGulieva@fa.ru

Резюме: Уже начиная с создания парового двигателя существует давняя традиция регулировать использование технологических инноваций в обществе с помощью правовых средств и инструментов. Государственное регулирование может обеспечить признание конкретной технологии, установить стандарты, которые могут помочь технологии быть принятой обществом, и определить критерии, при которых её использование является приемлемым. Таким образом, регулирование оказывает большое влияние на развитие инноваций и степень внедрения технологий в определённые области. Сегодня многие страны, такие как Россия, Соединённые Штаты Америки, государства – члены Европейского Союза и многие другие, разрабатывают механизм по государственному регулированию технологических инноваций, включая искусственный интеллект (далее – ИИ). Искусственный интеллект является основой для многих приложений, таких как чат-боты, интеллектуальные помощники и устройства по распознаванию лиц. Именно последнее свойство ИИ вызывает наибольшее количество споров как в обществе, так и в научной среде, что особенно связано с вопросом защиты персональных данных.

Ключевые слова: персональные данные, правовое регулирование, технологии, искусственный интеллект, государство, защита

Для цитирования: Гулиева М.Э. Сравнительно-правовой анализ вопросов защиты персональных данных в процессе развития искусственного интеллекта. *США & Канада: экономика, политика, культура.* 2023; 53 (4): 108–117.
DOI: 10.31857/S2686673023040089 EDN: VGRGGY

Comparative Legal Analysis of Personal Data Protection in the Process of Artificial Intelligence Development

M.E. Gulieva

Financial University under the Government of the Russian Federation.
49/2, Leningradsky Prospekt, Moscow, 125993, Russian Federation.
Researcher ID: HPD-5668-2023 Scopus Author ID: 57224857847 РИНЦ ID: 1012999
ORCID: 0000-0002-3961-0135 e-mail: MEGulieva@fa.ru

Abstract: Since the creating of steam engine, there has been a long tradition of regulating the use of technological innovation in society through legal methods and instruments. Government regulation can provide recognition for a particular technology, set standards that can help a technology be accepted by society, and define criteria under which the use of that technology is acceptable. Thus, regulation has a great influence on the development of innovations and the extent to which technologies are introduced into certain areas. Today, many states, like Russia, the United States of America, state-members of the European Union and many others are developing a mechanism for state regulating technological innovations, including artificial intelligence (called as AI). Artificial intelligence is the basis for many applications such as chatbots, smart assistants, and facial recognition devices. The last feature of AI causes the most controversy argues both in society and in the scientific community. The topic of privacy and protection of personal data especially raises very many questions.

Keywords*:* personal data, legal regulation, artificial intelligence, state, protection

For citation: Gulieva, M.E. Comparative Legal Analysis of Personal Data Protection in the Process of Artificial Intelligence Development. *USA & Canada: Economics, Politics, Culture*. 2023; 53 (4): 108-117. DOI: 10.31857/S2686673023040089
EDN: VGRGGY

ВВЕДЕНИЕ

Развитие цифровых технологий не только ввело много нововведений в жизнь обычных граждан, но также заставило государства задуматься о возможных рисках и последствиях применения этих самых технологий на практике. Наиболее актуальным вопросом наравне с возможностью регулирования деятельности информационных технологий стал вопрос о защите персональных данных. Персональные данные пользователей зачастую становятся самой уязвимой статьёй цифровизации по причине недоработанности пунктов, связанных с обеспечением безопасности личной информации.

На национальном и международном уровне принимаются многочисленные нормативно-правовые акты, направленные на обеспечение основных прав и свобод человека и гражданина, закрепляя различные механизмы защиты этих самых прав и свобод. Но цифровизация современных производственных процессов, как и применение высокотехнологичных процессов практически во всех социальных сферах, приводит к вопросу о защите персональных данных. Становясь частью цифрового пространства, человек предоставляет доступ к информации о частной жизни всё более широкому кругу лиц и этим самым подвергает себя большим рискам. Персональные данные физического лица необходимо ограждать от третьих лиц вследствие увеличения роста краж персональной информации, так как, оказавшись в руках правонарушителя, такие данные превращаются в поражающее оружие против личности [Давыдова О.Б., 2018].

РОССИЙСКАЯ ФЕДЕРАЦИЯ

Основополагающим элементом в механизме защиты персональных данных является его достаточная нормативно-правовая обеспеченность. Законодательство Российской Федерации на всех уровнях регулирует вопросы защиты персональных данных. Так, Конституция РФ в статье 23 устанавливает, что каждый человек имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а в статье 24 говорится, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются [1]. Дальнейшее развитие института персональных данных в Российской Федерации проявилось в принятии федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Считается, что указанный закон является важным шагом к повышению уровня безопасности хранения и обработки персональных данных российских граждан; снижается вероятность несанкционированного получения доступа к информации иностранными лицами. Согласно статье 3 федерального закона «О персональных данных», под персональными данными понимается любая информация, которая может прямо или косвенно относиться к физическому лицу. Также, согласно закону, то, что является персональными данными или личной информацией, может видоизменяться в зависимости от того, можно ли идентифицировать самого человека или как его можно разумно идентифицировать при определённых обстоятельствах [2]. В дополнение к общим персональным данным необходимо учитывать, прежде всего, специальные категории персональных данных (также известные как конфиденциальные персональные данные), которые имеют большое значение, поскольку они подпадают под более высокий уровень защиты. Эти данные включают генетические, биометрические характеристики и информацию о состоянии здоровья, а также личные данные, раскрывающие расовое и этническое происхождение, политические взгляды, религиозные или идеологические убеждения или членство в профсоюзах [Рассолов И.М., Чубукова С.Г., Микурова И.В., 2019].

И последняя, но не менее важная особенность этого закона в том, что информация должна относиться к физическому лицу. Другими словами, защита данных не распространяется на информацию о юридических лицах, таких как общества, корпорации, фонды и учреждения. Напротив, для физических лиц защита начинается и прекращается с наличием правоспособности. По сути, человек получает эту способность при рождении и теряет её после смерти. Поэтому данные должны быть присвоены идентифицированным или идентифицируемым живым людям, чтобы считаться «личными».

Правила защиты данных меняются в зависимости от страны, региона, отрасли; это означает, что вопросы правового регулирования ИИ в области персональных данных можно решать по-разному, на основе местного, национального

или международного законодательства [Незнамов А.В., Волынец А.Д., Бакуменко В.В., 2018]. На сегодняшний день государственные стратегии по применению ИИ, включая вопросы защиты персональных данных, разработаны во многих странах мира, таких как США, Канада, государства – члены Европейского Союза и многие другие. Рассмотрим некоторые из них.

СОЕДИНЁННЫЕ ШТАТЫ АМЕРИКИ

В США вопросы конфиденциальности данных вызывают бурные общественные дискуссии. Многочисленные споры, вызванные новыми изменениями в законодательстве в результате распространения коронавирусной инфекции, показали сильную обеспокоенность по поводу защиты персональных данных. О серьёзности ситуации свидетельствует тот факт, что был принят ряд контрмер, которые могут значительно ограничить возможность использования технологий искусственного интеллекта компаниями для решения задач, в том числе связанных с самим коронавирусом. В частности, ограничения на деятельность технологии по распознаванию лиц и персональных медицинских данных могут препятствовать внедрению технологий для отслеживания распространения и воздействия вируса, таких как применение теплового сканирования для допуска сотрудников на свои рабочие места (эта технология может также применять сканирование лица сотрудника). В свою очередь, владельцы крупной жилой недвижимости рассматривают возможность использования технологии распознавания лиц для контроля и наблюдения за входами в свои здания и предотвращения проникновения посторонних лиц, которые могут быть переносчиками коронавирусной инфекции.

Законопроекты, представленные на рассмотрение Конгрессу США, которые устанавливали бы требование на наличие согласия на использование технологии распознавания лиц, не прошли даже первичный этап. Тем не менее, что касается государственных организаций, один законопроект, который в настоящее время находится на рассмотрении Конгресса, выходит за рамки наложения требования о согласии, а вместо этого просто запрещает применение процесса распознавания лиц и других биометрических технологий федеральными организациями. Кроме того, данный законопроект регулирует вопрос финансирования федеральных грантов местными и государственными организациями, а также вводит мораторий на технологию распознавания лиц и предоставляет право на подачу иска лицам, чьи данные были собраны или использованы в нарушение данного закона.

Одной из наиболее распространённых сфер применения искусственного интеллекта в США, как известно, является именно сфера здравоохранения. Так, закон «Об умном наблюдении» (*Smartwatch*) запрещает компаниям передавать или продавать информацию о состоянии здоровья с личных потребительских устройств без информированного согласия заказчика, включая носимые устрой-

ства и трекеры [3]. Некоторые представители академической среды призвали к регулированию вопросов защиты медицинских или личных данных, в том числе, чтобы обработка этой информации соответствовала правилам, установленным законом «О переносимости и подотчётности медицинского страхования» от 1996 г. (далее – *HIPAA*) [4], в ещё более строгом порядке.

А данные, подпадающие под действие самого *HIPAA,* будут регулироваться его «Правилом конфиденциальности» [5], которое также может непреднамеренно препятствовать развитию технологий ИИ. Например, один из основных принципов «Правила конфиденциальности» заключается в том, что использование и раскрытие защищённой медицинской информации должно быть ограничено только «минимумом, необходимым для выполнения конкретной транзакции или действия». Такие ограничения на использование могут повлиять и на возможность разработки искусственного интеллекта, связанного со сферой здравоохранения, так как использование ИИ в сфере здравоохранения находится под пристальным общественным вниманием. Так, например, медицинские работники некоторых штатов недавно подали иск в отношении компании, производящей бытовое устройство с голосовым управлением, утверждая, что оно незаконно записывало, хранило и анализировало информацию о пациентах, защищённую *HIPAA,* включая взаимодействие между медицинскими работниками и их пациентами [4].

Возможно, ни одна область применения технологии искусственного интеллекта не вызывала таких горячих усилий по регулированию или запрету её использования в Соединённых Штатах, как внедрение технологии распознавания лиц правоохранительными органами и чиновниками иных государственных ведомств. Как и другие биометрические показатели, данные, связанные с геометрией и структурой лица, часто считаются одними из «самых личных» и конфиденциальных данных о человеке, что побуждает правозащитников призывать к особой бдительности при защите от несанкционированного или злонамеренного использования. В результате многие общественные группы и другие ярые противники технологии распознавания лиц поспешили забить тревогу из-за проблем, связанных с базовой технологией, а также о потенциальном или фактическом неправомерном использовании со стороны государственных органов, хотя большая часть регулирующей деятельности на сегодняшний день осуществлялась на местном уровне. Несмотря на все эти усилия по ограничению применения технологии распознавания лиц, её использование фактически увеличилось в 2021 г., в первую очередь из-за усилий правоохранительных органов по выявлению и аресту участников беспорядков в здании Капитолия США. Однако даже повсеместное осуждение участников беспорядков коренным образом не изменило «тревожное» отношение защитников цифровых прав к растущему применению технологий распознавания лиц [6].

Обеспокоенность по поводу распознавания лиц и других биометрических технологий, выдвинутая на передний план движениями за расовую справедли-

вость, заставила законодательные органы федерального уровня и штатов пересмотреть использование технологии распознавания лиц государственными и полицейскими управлениями и предложить закон, запрещающий применение этой технологии полицией в целом. Так, предлагаемый закон «О развитии технологии распознавания лиц» [7] призывает министра торговли и Федеральную торговую комиссию провести исследование технологии распознавания лиц, а предлагаемый закон «О развитии американского ИИ» [8] будет способствовать формированию отношения к искусственному интеллекту «в соответствии с принципом защиты частной жизни, гражданских прав и свобод». Однако, несмотря на возобновление внимания к проблеме технологии распознавания лиц и сбора и использования биометрических данных в течение последних нескольких лет, Конгресс ещё не принял ни одного из предложенных законов [9]. Единственным действующим на федеральном уровне можно считать закон «О защите персональных данных» от 1980 года [10].

За последние несколько лет законодатели на уровне штатов сами разработали несколько законопроектов, связанных с защитой персональных данных. Среди них, к примеру, можно отметить, закон штата Калифорния «О правах на неприкосновенность частной жизни и обеспечении их соблюдения». Хотя большинство из них не относятся конкретно к технологиям ИИ, некоторые включают положения, касающиеся автоматизированного принятия решений, а большая часть из них может сильно повлиять на сам процесс развития технологий ИИ в Соединённых Штатах.

КАНАДА

Канадское правительство и промышленность в целом за последние несколько лет инвестировали значительные средства в развитие сферы ИИ, в развитие сотрудничества с целью создания инновационных и исследовательских центров. Кроме того, для расширения этой сферы были выделены гранты в размере нескольких миллионов долларов. Канада не только оказала заметное влияние на развитие в глобальных масштабах различных инноваций в области ИИ, разработав динамичную стартап-экосистему, но также способствовала привлечению экспертов в этой области, в том числе исследователей в крупные компании – разработчики программного обеспечения.

Единственным нормативно-правовым актом всестороннего регулирования ИИ и автоматизированных систем в Канаде является Директива правительства Канады об автоматизированной системе поддержки принятия решений (“*Canada’s Directive on Automated Decision-making*” либо *“Canada ADM Directive”)* (далее – директива). Она вступила в силу 1 апреля 2020 г. В отличие от предлагаемых в отношении ИИ норм в Европейском Союзе, канадская директива *“ADM”* очень ограничена по своему охвату. Что наиболее важно, директива “ADM” регулирует только системы федерального правительства и федеральные структу-

ры. Она не применяется к системам, используемым правительствами провинций, муниципалитетами или провинциальными агентствами, таким как полицейские службы, агентства по защите детей, а также многим другим важным государственным учреждениям. Канадская директива также не применяется к системам искусственного интеллекта или нормативным актам, относящимся к частному сектору.

Директива устанавливает базовые требования, применяемые обычно ко всем системам ИИ, независимо от уровня их влияния [11: s. 6], в том числе: к доступу, анализу информации, тестированию и аудиту для лицензионного программного обеспечения; к выпуску пользовательского исходного кода, принадлежащего правительству Канады; к обеспечению качества и к мониторингу, включая:

– тестирование «перед запуском в производство… [чтобы убедиться, что все системы] проверены на непреднамеренные искажения данных и другие факторы, которые могут исказить результаты»;

– мониторинг «результатов систем для защиты от непредсказуемых последствий» и проверка «соблюдения институционального и программного законодательства»;

– консультации с государственными юридическими службами с целью обеспечения соблюдения требований директивы действующему законодательству;

– предоставление информации об эффективности и результативности и другие.

Директива устанавливает требования по алгоритмической оценке воздействия для каждого автоматизированного процесса «Поддержки принятия решений», включая также оценку «воздействия на права отдельных лиц или сообщества в целом». В директиве также указывается, что мониторинг и проверки должны быть публичными и открытыми.

Канадская директива прямо не требует, чтобы системы ИИ или иные автоматизированные системы соответствовали Хартии Европейского Союза об основных правах или канадскому законодательству о правах человека. Напротив, в директиве говорится, что её целью является «гарантировать, чтобы автоматизированные системы “Поддержки принятия решений” были развёрнуты таким образом, чтобы снизить риски для канадцев и федеральных учреждений, и вести к более эффективному, точному, последовательному и интерпретируемому процессу, соответствующему канадскому законодательству» [11: s. 4.1].

Как указано в директиве, её цель состоит в том, чтобы «положения, принятые ведомством федерального правительства, были правомерны и соблюдали принцип процедурной справедливости и процессуальные требования». Разработка и внедрение искусственного интеллекта представляет собой многогранный процесс, включающий различные аспекты, и государство должно определять уровни рисков, которые могут иметь различные организации и предприятия.

ЗАКЛЮЧЕНИЕ

Таким образом, завершая тему правового обеспечения защиты персональных данных, можно сделать следующие выводы.

– При использовании технологий ИИ важно сохранять прозрачность и открытость, чтобы пользователи могли интерпретировать выходные данные и применять их надлежащим образом. Данное положение может быть включено в руководство по использованию ИИ в отношении предприятий, чтобы не допускать неправильного толкования. Многие технологии искусственного интеллекта непредсказуемы и трудно поддаются контролю. Должна быть осуществлена предварительная оценка рисков, а также проведена проверка того, что системы ИИ работают точно на протяжении всей фазы их жизненного цикла с воспроизводимыми результатами. Кроме того, системы ИИ должны адекватно обрабатывать ошибки, имея возможности, в том числе, для их исправления. Также следует разработать дополнительные правила для обеспечения устойчивости к кибератакам и попыткам манипулирования данными или алгоритмами.

– Важен также контроль со стороны человека, в дополнение к тому, что уже установлено для поддержки автоматизированного принятия решений. В зависимости от обстоятельств человеческий контроль должен осуществляться до того, как будут получены результаты, или после и/или на протяжении всего процесса обучения и получения результатов. Это будет зависеть также от типа системы и сферы её использования.

– Дополнительные требования могут быть установлены для других конкретных систем, включая дистанционную биометрическую идентификацию, которая позволяет идентифицировать людей на расстоянии и в общественном месте с помощью набора биометрических идентификаторов (например, отпечатков пальцев, изображения лица и т.д.), которые сравниваются с другой информацией, хранящейся в базе данных.

ИСТОЧНИКИ

1. Конституция Российской Федерации от 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года.

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ (в редакции от 25 июля 2011 г.) «О персональных данных». Доступ из справочно-правовой системы «Консультант плюс» (accessed 16.01.2023).

3. Stop Marketing and Revealing the Wearables and Trackers Consumer Health Data Act, S. 500, 117th Cong. (2021).

4. Mason Marks. Emergent Medical Data: Health Information Inferred by Artificial Intelligence, 11 U.C. Irvine L. Rev. 995 (2021). Available at:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3554118 (accessed 16.01.2023).

5. Health Insurance Portability and Accountability Act, 45 CFR section 264(a)-(b) (2006).

6. Drew Harwell & Craig Timberg. How America's Surveillance Networks Helped the FBI Catch the Capitol Mob // *The Washington Post*. April 2, 2021. Available at: https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy (accessed 16.01.2023).

7. Advancing Facial Recognition Technology Act, H.R. 4039, 117th Cong. (2021).

8. Advancing American AI Act, S. 1353, 117th Cong. (2021).

9. Nicole Sakin. Will there be federal facial recognition regulation in the US? // IAPP, February 11, 2021. Available at: https://iapp.org/news/a/u-s-facial-recognition-roundup/ (accessed 16.01.2023).

10. Privacy Protection Act of 1980. Available at: https://www.justice.gov/archives/jm/criminal-resource-manual-661-privacy-protection-act-1980 (accessed 16.01.2023).

11. Canada's Directive on Automated Decision-making. (Canada ADM Directive). 2019. Available at: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (accessed 16.01.2023).

СПИСОК ЛИТЕРАТУРЫ

Незнамов А.В., Волынец А.Д., Бакуменко В.В. 2018. Новые законы робототехники. Регуляторный ландшафт. Мировой опыт регулирования робототехники и технологий искусственного интеллекта. Под ред. А.В. Незнамова. Москва, Инфотропик. 220 с. ISBN 978-5-9998-0324-5.

Давыдова О.Б. 2018. Защита персональных данных. *Вестник науки и образования*. № 6 (42). С. 89–90.

Рассолов И.М., Чубукова С.Г., Микурова И.В. 2019. Биометрия в контексте персональных данных и генетической информации: правовые проблемы. *Lex russica (Русский закон).* №1 (146). С. 108–118. DOI: 10.17803/1729-5920.2019.146.1.108-118

REFERENCES

Neznamov, A.V., Volynets, A.D., Bakumenko, V.V. 2018. Novye zakony robototekhniki. Reguliatornyi landshaft. Mirovoi opyt regulirovaniia robototekhniki i tekhnologii iskusstvennogo intellekta [New Laws of Robotics. Regular Landscape. World Experience in Regulating of Robotics and Artificial Intelligence Technologies] (In Russ.). Ed. by A.V. Neznamov. Moscow: Infotropik. 220 p. ISBN 978-5-9998-0324-5.

Davidova, O.B. 2018. Zashchita personal'nykh dannykh [Protection of Personal Information] (In Russ.). *Vestnik nauki i obrazovaniya*. No. 6 (42). P. 90.

Rassolov, I.M., Chubukova, S.G., Mikurova, I.V. 2019. Biometriia v kontekste personal'nykh dannykh i geneticheskoi informatsii: pravovye problemy [Biometrics in the Context of Personal Data and Genetic Information: legal issues] (In Russ.). *Lex Russica.* No.1 (146). P. 108-118. (In Russ.). DOI: 10.17803/1729-5920.2019.146.1.108-118

ИНФОРМАЦИЯ ОБ АВТОРЕ / INFORMATION ABOUT THE AUTHOR

ГУЛИЕВА Мехрибан Эльбрус кызы, кандидат юридических наук, доцент Департамента международного и публичного права Юридического факультета Финансового университета при Правительстве Российской Федерации.
Российская Федерация, 125993, Москва, Ленинградский проспект, д. 49/2.

GULIEVA Mekhriban Elbrus kyzy, Candidate of Sciences (Law), Associate Professor of the Department of International and Public Law of the Law Faculty of the Financial University under the Government of the Russian Federation.
49/2, Leningradsky Prospekt, Moscow, 125993, Russian Federation

Статья поступила в редакцию / Received 19.01.2023.
Поступила после рецензирования / Revised 30.01.2023.
Статья принята к публикации / Accepted 1.02.2023.