УДК 004.738.5
ББК Х401.114
DOI: 10.14529/law200313

ПРОБЛЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ И ЦИФРОВОГО ПРОФИЛЯ ЧЕЛОВЕКА В СЕТИ ИНТЕРНЕТ В УСЛОВИЯХ ПАНДЕМИИ

А. В. Минбалеев[1,2], В. А. Филоненкова[1]
[1] Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва,
[2] Южно-Уральский государственный университет, г. Челябинск

Статья посвящена исследованию проблем защиты персональных данных и цифрового профиля человека в условиях пандемии. В условиях развития в России и во всем мире пандемии коронавируса COVID-19 очень серьезной проблемой является необходимость обеспечения и защиты персональных данных, в первую очередь о состоянии здоровья граждан, а также данных, которые государства получают в результате контроля за гражданами и соблюдением ими режима самоизоляции, социального дистанцирования и иных противоэпидемиологических мер, которые вводит государство в борьбе с пандемией. Особая опасность связана с тем, что большая часть таких данных размещается в сети Интернет, в связи с чем возникают значительные риски того, что эта информация может быть незаконно получена с помощью хакерских атак и незаконно распространена.

Социальный скоринг часто основывается на использовании технологий big data и искусственного интеллекта. В этом случае искусственный интеллект обрабатывает огромное количество данных клиентов, анализирует их социальные характеристики и на основе этих больших данных ранжирует пользователей. Делается вывод о том, что компании, планирующие такое использование персональных данных, должны в качестве специальной цели обработки уведомлять Роскомнадзор, выделять данную цель в процессе обработки персональных данных и получать специальное согласие субъектов персональных данных на такое согласие.

Ключевые слова: персональные данные, цифровой профиль, пандемии, социальный скоринг, искусственный интеллект, защита.

Обработка персональных данных в сети Интернет в условиях глобального информационного общества и цифровизации все чаще связывается с активным использованием информационных и цифровых технологий[1]. Часто для обработки персональных данных в сети Интернет используются технологии искусственного интеллекта (далее – ИИ), позволяющие на основе сформированного алгоритма выстроить систему эффективного анализа большого объема персональных данных и принятия быстрых решений, которые часто даже не позволяют получить согласие субъекта персональных данных на подобное использование. Высокая скорость и значительные объемы обрабатываемых персональных данных с использованием ИИ не позволяют достаточно оперативно учесть согласие субъекта. Кроме того, использование ИИ часто сопровождается достаточно большим количеством ошибок и сбоев, что приводит к нарушениям прав субъектов персональных данных.

В связи с этим сегодня важно внесение изменений в законодательство о персональных данных, важно предусмотреть специальное согласие субъекта персональных данных в случаях их обработки, в том числе в сети Интернет, с использованием искусственного интеллекта, робототехники и киберфизических систем.

С точки зрения защиты персональных данных с использованием технологий ИИ и больших данных основные вопросы касаются, с одной стороны, объема и разнообразия обрабатываемых персональных данных, а с дру-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта конкурса А № 20-011-00077 «Правовое регулирование цифрового профиля человека в сети «Интернет».

гой самой обработки и ее результатов. Внедрение сложных алгоритмов и программного обеспечения для преобразования массовых данных в ресурс для целей принятия решений затрагивает в частности отдельных лиц и группы лиц, особенно в случаях профилирования или маркировки, и, в конечном итоге, вызывает много проблем с защитой данных. Большие данные и ИИ поднимают несколько вопросов в отношении идентификации контроллеров и процессоров, а также их ответственности: когда собирается и обрабатывается такой большой объем данных, кто является владельцем этих данных? Когда данные обрабатываются машинами разведки и программным обеспечением, кто является контроллером? Каковы точные обязанности каждого участника процесса обработки? А для каких целей могут использоваться большие данные?

Вопрос об ответственности в контексте ИИ становится все более сложным, когда ИИ принимает решение, основанное на обработке данных, которые он сам разработал. ИИ и автоматизированное принятие решений вызывают вопросы о том, кто несет ответственность за нарушения, затрагивающие конфиденциальность субъектов данных, где сложность и объем обрабатываемых данных не могут быть определены с уверенностью. В тех случаях, когда ИИ и алгоритмы рассматриваются как продукты, возникает проблема между личной ответственностью и ответственностью за продукт [1].

Сегодня явно существует необходимость специального регулирования процедур обработки персональных данных в сети Интернет при осуществлении сбора и обработке персональных данных из социальной сетей и иных источников для социального скоринга. Социальный скоринг представляет собой разновидность скоринга, при котором происходит оценивание клиента на основании его социальных характеристик и прогнозирование его дальнейшего поведения на основе ряда действий в сети Интернет, социальных сетях. Потребители-пользователи сети Интернет постоянно оставляют свои «следы», осуществляя те или иные покупки, интересуясь определенными сайтами, проявляя определенные интересы.

Оперируя в сети Интернет и социальных сетях такими данными, как пол, возраст, место проживания, должность, хобби, спортивные интересы и другие, граждане присваивают определенные ранги, уровни, социальные статусы и характеристики. На основании этого клиенты либо рассматриваются в качестве надежных, представляющих интерес, выгодных, а часть попадают в группу, к которой у компании нет интереса. Такие группы могут подвергаться отключениям, блокированию доступа, исключению из числа пользователей и т.п. [2].

Социальный скоринг часто основывается на использовании технологий big data и искусственного интеллекта. В этом случае ИИ обрабатывает огромное количество данных клиентов, анализирует их социальные характеристики и на основе этих больших данных ранжирует пользователей.

Нам представляется, что компании, планирующие такое использование персональных данных, должны в качестве специальной цели обработки уведомлять Роскомнадзор, выделять данную цель в процессе обработки персональных данных и получать специальное согласие субъектов персональных данных на такое согласие.

В условиях развития в России и во всем мире пандемии коронавируса COVID-19 очень серьезной проблемой является необходимость обеспечения и защиты персональных данных, в первую очередь о состоянии здоровья граждан, а также данных, которые государства получают в результате контроля за гражданами и соблюдением ими режима самоизоляции, социального дистанцирования и иных противоэпидемиологических мер, которые вводит государство в борьбе с пандемией. Особая опасность связана с тем, что большая часть таких данных размещается в сети Интернет, в связи с чем возникают значительные риски того, что эта информация может быть незаконно получена с помощью хакерских атак и незаконно распространена.

Поэтому в мире принимаются достаточно интересные решения в этой сфере. Так, Исполнительный комитет Всемирной ассамблеи по защите неприкосновенности частной жизни (GPA) признал беспрецедентными проблемы, с которыми сталкиваются при решении проблемы распространения коронавируса COVID-19, и сделал официальное заявление, которое поддержали национальные правительства и омбудсмены всех стран-членов Всемирной ассамблеи по защите неприкосновенности частной жизни (GPA). В заявлении в частности указывается, что «решение этих

проблем требует скоординированных действий на национальном и глобальном уровнях, включая обмен необходимой личной информацией между организациями и правительствами, а также трансграничный обмен информацией. Мы уверены, что требования по защите данных не остановят важнейший обмен информацией в поддержку усилий по борьбе с этой глобальной пандемией. Универсальные принципы защиты данных во всех наших законах позволят использовать данные в общественных интересах и по-прежнему обеспечивают защиту, которую ожидает общественность. Органы защиты данных готовы помочь в обеспечении быстрого и безопасного обмена данными для борьбы с COVID-19. Данные здравоохранения считаются чувствительными во многих юрисдикциях, но работа между органами по защите данных и правительствами означает, что мы уже видели много примеров национальных подходов к обмену сообщениями общественного здравоохранения, использования новейших технологий для содействия безопасным и быстрым консультациям и диагнозам, создания связей между системами общественных данных для облегчения идентификации распространения вируса» [3].

Можно выделить следующие ключевые направления, требующие повышенного внимания органов, осуществляющих контроль за соблюдением законодательства о персональных данных:

– защита обеспечения персональных данных о здоровье граждан, получаемых в процессе оказания медицинской помощи, забора проб клинического материала, а также лечения больных коронавирусом;

– защита персональных данных в режиме больших данных, полученных в рамках контроля и слежения за гражданами в период пандемии.

Многие государства сегодня с большой осторожностью относятся к проблемам защиты персональных данных, в том числе в сети Интернет, в условиях коронавируса COVID-19.

Одним из наиболее серьезных механизмов, обеспечивающих защиту прав субъектов персональных данных, в том числе в сети Интернет, является австралийская система защиты персональных данных. Управление австралийского комиссара по вопросам информации (OAIC) является независимым органом, созданным для обеспечения поддержания конфиденциальности и прав на доступ к информации. На него возложено ряд обязанностей и полномочий. Управление австралийского комиссара по информации (OAIC) отмечает, что закон о конфиденциальности не запрещает обмен критически важной информацией для управления распространением коронавируса. Государственные организации и частные компании (включая частных поставщиков медицинских услуг) имеют важные обязательства по поддержанию безопасного рабочего места для персонала и посетителей и соответствующим образом обрабатывают личную информацию. Для того чтобы справиться с пандемией, соблюдая конфиденциальность, OAIC рекомендует организациям стремиться ограничить сбор, использование и раскрытие личной информации особенно в сети Интернет тем, что необходимо для предотвращения и управления COVID-19. Они также должны принять разумные меры для обеспечения безопасности личной информации, в том числе личной информации сотрудников и членов их семей, посетителей помещений организации, клиентов, пользователей и широкой общественности. Там, где требуются изменения в рабочих механизмах, организации также должны рассмотреть потенциальное воздействие на обработку и безопасность личной информации, оценить любые риски и разработать стратегии смягчения последствий. В ходе обработки персональных данных только минимальный объем личной информации, разумно необходимый для предотвращения или управления COVID-19, должен быть собран, использован или раскрыт, должна быть рассмотрена возможность принятия мер уже сейчас, чтобы уведомить сотрудников о том, как их организация будет обрабатывать информацию в ответ на любой потенциальный или фактический случай COVID-19 на рабочем месте. Важно убедиться, что приняты разумные меры для обеспечения безопасности личной информации, в том числе в тех случаях, когда сотрудники работают удаленно через сеть Интернет. Закон о конфиденциальности не запрещает сотрудникам работать удаленно в ответ на COVID-19, однако австралийские принципы конфиденциальности будут по-прежнему применяться [4].

Очень часто персональные данные собираются через мобильные приложения, специальные сайты и цифровые платформы. Управ-

ление австралийского комиссара по информации (OAIC) в этой связи указывает, что цель, для которой объект приложения собирает личную информацию, называется основной целью сбора. Это конкретная функция или деятельность, для которой организация собирает личную информацию. Если организация-приложение использует или раскрывает личную информацию для другой цели, это называется вторичной целью. В отношении COVID-19 как инфекционного заболевания цель сбора личной информации от сотрудника или посетителя заключается в предотвращении или управлении риском заражения COVID-19 для обеспечения того, чтобы необходимые меры предосторожности могли быть приняты в отношении этого лица и любых других лиц, которые могут подвергаться риску. В этих обстоятельствах личная информация может быть использована или раскрыта только для этой цели, поскольку она относится к основной цели сбора. Любое другое использование или раскрытие информации будет являться вторичной целью, и операторам персональных данных необходимо выяснять, не является ли обработка официальным ограничением, например, возможностью вторичного использования, когда оно требуется или разрешается в соответствии с австралийским законодательством или когда получение согласия неразумно или нецелесообразно в связи с необходимостью уменьшить или предотвратить серьезную угрозу жизни, здоровью или безопасности любого лица или общественному здоровью или безопасности [5].

Еще в качестве одного из последних примеров организации защиты персональных данных в условиях пандемии можно привести достаточно мало известную в юридических исследованиях систему защиты персональных данных в Албании. Здесь Уполномоченный по защите персональных данных также выработал определенные рекомендации по защите персональных данных. В документе в частности отмечается, что, «учитывая беспрецедентную национальную и международную ситуацию, сложившуюся в результате пандемии коронавируса COVID-19, а также со ссылкой на ряд вопросов, рассмотренных в этот период государственными, частными операторами и заинтересованными гражданами в связи с воздействием и последствиями обработки персональных данных в этих конкретных условиях, Управление уполномоченного по информации и защите данных считает целесообразным предусмотреть некоторые руководящие принципы в обобщенном виде, поиск справедливого и разумного толкования законодательства о защите персональных данных в контексте мер, осуществляемых для предотвращения и последующего смягчения серьезных угроз, вызванных распространением вируса COVID-19 в Албании.

Управление уполномоченного призывает граждан осознать необходимость и важность обработки персональных данных, направленной на успешное преодоление и предотвращение негативных последствий, порождаемых COVID-19, и заверяет их в своей приверженности решению любых вопросов, поднятых сторонами, участвующими в этой коллективной борьбе за права человека [6].

Наряду с необходимостью обеспечения защиты прав на персональные данные в условиях пандемии допускаются определенные ограничения, обусловленные необходимостью защиты прав и законных интересов граждан на здоровье, а также защиты общества от угрозы пандемии. В этой связи вполне оправдано на период пандемии расширить возможности обработки персональных данных, в том числе в информационно-телекоммуникационных сетях и сети Интернет, без согласия субъекта персональных данных. Однако данные меры должны быть привязаны к официальному состоянию режима повышенной готовности или чрезвычайному режиму, носить временный характер и после окончания отменены.

Литература/References

1. Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018. 2018 edition. 402 p. Available at: fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

2. Available at: www.statsoft.ru.

3. Statement by the GPA Executive Committee on the Coronavirus (COVID-19) pandemic. Available at: globalprivacyassembly.org/gpaexco-covid19/.

4. Privacy advice for the COVID-19 pandemic. Available at: www.oaic.gov.au/updates/news-and-media/privacy-advice-for-the-covid-19-pandemic/.

5. Coronavirus (COVID-19): Understanding your privacy obligations to your staff. Available at: www.oaic.gov.au/privacy/guidance-and-

advice/coronavirus-covid-19-understanding-your-privacy-obligations-to-your-staff/.

6. Guidelines on the protection of personal data in the context of the measures taken against COVID-19. Available at: www.idp.al/2020/03/20/guidelines-on-the-protection-of-personal-data-in-the-context-of-the-measures-taken-against-covid-19/?lang=en.

Минбалеев Алексей Владимирович – доктор юридических наук, профессор, заведующий кафедрой информационного права и цифровых технологий, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва, профессор кафедры теории государства и права, конституционного и административного права, Южно-Уральский государственный университет, г. Челябинск. E-mail: alexmin@bk.ru.

Филоненкова Валерия Александровна – магистрант кафедры информационного права и цифровых технологий, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), г. Москва. E-mail: filonenkova.1996@mail.ru.

Статья поступила в редакцию 27 июня 2020 г.

DOI: 10.14529/law200313

PROBLEMS OF PERSONAL DATA PROTECTION AND A DIGITAL PROFILE OF A PERSON ON THE INTERNET IN THE CONTEXT OF A PANDEMIC

A. V. Minvaleev[1,2], V. A. Filonenkova[1]

[1] Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

[2] South Ural State University, Chelyabinsk, Russian Federation

The article is devoted to the study of the problems of personal data protection and digital profile of a person in the context of a pandemic. In the context of the development of the COVID-19 coronavirus pandemic in Russia and around the world, a very serious problem is the need to ensure and protect personal data, primarily about the health of citizens, as well as the data that States receive as a result of monitoring citizens and observing the regime of self-isolation, social distancing and other anti-epidemic measures that the state introduces in the fight against the pandemic. A particular danger stems from the fact that the majority of this data is posted on the Internet, in connection with which there are significant risks that this information could be illegally obtained through hacking and illegally distributed.

Social scoring is often based on the use of big data and artificial intelligence technologies. In this case, artificial intelligence processes a huge amount of customer data, analyzes their social characteristics, and ranks users based on this big data. It is concluded that companies planning such use of personal data should notify Roskomnadzor as a special purpose of processing, highlight this purpose in the process of processing personal data and obtain special consent of personal data subjects for such consent.

Keywords: personal data, digital profile, pandemics, social scoring, artificial intelligence, protection.

Aleksey Vladimirovich Minbaleev – Doctor of Sciences (Law), Professor, head Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Moscow, Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University, Chelyabinsk, Russian Federation. E-mail: alexmin@bk.ru.

Valeria Aleksandrovna Filonenkova – master's student at the Department of Information Law and Digital Technologies, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation. E-mail: filonenkova.1996@mail.ru.

Received 27 June 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Минбалеев, А. В. Проблемы защиты персональных данных и цифрового профиля человека в сети интернет в условиях пандемии / А. В. Минбалеев, В. А. Филоненкова // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 3. – С. 89–94. DOI: 10.14529/law200313.

FOR CITATION

Minvaleev A. V., Filonenkova V. A. Problems of personal data protection and a digital profile of a person on the internet in the context of a pandemic. *Bulletin of the South Ural State University. Ser. Law*, 2020, vol. 20, no. 3, pp. 89–94. (in Russ.) DOI: 10.14529/law200313.