УДК 342. 423
ББК Х.400.114
DOI: 10.14529/law200214

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЦИФРОВОГО ПРОФИЛИРОВАНИЯ ДЕЯТЕЛЬНОСТИ ЧЕЛОВЕКА

А. К. Жарова
Институт государства и права РАН, г. Москва

Распространение систем, анализирующих большие объемы данных и их глубокое проникновение в различные области жизнедеятельности человека, требует исследования возникающих правовых проблем. В связи с этим закономерен вопрос – где же черта между правовыми последствиями, создаваемыми анализом больших объемов данных, и уже ставшими традиционными формами оформления согласия и использования данных. В статье исследована проблема правового обеспечения требований об информировании субъекта персональных данных при профилировании деятельности субъекта. Для этого исследовано российское законодательство, Евросоюза и Великобритании.

Без разработки правовых требований к обработке больших цифровых данных возможны ситуации вмешательства в частную жизнь лица, построение информационной модели профиля человека на данных, не соответствующих действительности, а также принятие решений, имеющих юридически значимые последствия на основании таких моделей.

Формирование цифрового профиля субъекта напрямую связано с информацией о человеке, и в этом случае необходимо определить правовое регулирование не только в отношении процедуры получения информированного согласия, но и надежности и достоверности источников данных, на основе которых формируется цифровой профиль человека, поскольку он создается именно с целью достоверной идентификации человека и его предпочтений.

Ключевые слова: Интернет вещей, искусственный интеллект, большие данные, профилирование.

Нынешний этап развития человечества связан с использованием информационных технологий[1] не только в целях ускорения процессов обмена информацией, облегчения взаимодействия, но и принятия решений на основе собранных цифровых данных, размещенных в различных информационных системах, информационно-телекоммуникационных сетях и инфраструктурах. Такая обработка цифровых данных позволяет создавать условия, благодаря которым посредством собранных данных возможны вмешательство в частную жизнь, построение информационной модели профиля человека на данных, не соответствующих действительности, а также принятие решений, имеющих юридически значимые последствия на основании таких моделей.

Распространение систем, анализирующих большие объемы данных, и их глубокое проникновение в различные области жизнедеятельности человека требуют исследования возникающих правовых проблем. В связи с этим, закономерен вопрос – где же черта между правовыми последствиями, создаваемыми анализом больших объемов данных, и уже ставшими традиционными формами оформления согласия и использования данных. Основное различие между технологиями заключается в способах получения информированного согласия субъекта персональных данных, чьи данные в дальнейшем становятся объектом обработки.

Таким образом, мы подходим к проблеме правового обеспечения требований об информировании субъекта персональных данных при обработке его данных технологиями больших данных. Данная проблема в государствах, реализующих технологии Интернет вещей, искусственного интеллекта, Больших данных в целях профилирования деятельности человека, стоит остро, поскольку реализовать требования законодательства о персональных данных об информировании челове-

[1] Статья подготовлена в рамках гранта РФФИ № А. 20-011-00077 «Правовое регулирование цифрового профиля человека в сети «Интернет».

ка при применении вышеуказанных технологий сложно. Для решения возникшей ситуации предлагается принятие новых нормативных требований к разрабатываемым технологическим решениям.

Большинство государств начало разработку правовых документов, регламентирующих порядок обработки цифровых данных и создания на их основе цифровых профилей. Так, 1 января 2020 г. вступил в силу закон Калифорнии о защите прав потребителей, в 2018 году вступили в силу нормативные акты (GDPR) – Регламент EU 2016/679 и Директива EU 2016/680, в которых определены регламенты профилирования на основе цифровых данных.

В июле 2019 года комитетом Государственной Думы по информационной политике, информационным технологиям и связи в Государственную думу Российской Федерации был внесен законопроект «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)», который предлагает определить инфраструктуру цифрового профиля гражданина. Минкомсвязи России подготовило законопроект «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)», сходный с вышеуказанным законопроектом, который также регламентирует отношения в области цифрового профилирования.

Обработка персональных данных в новых технологических условиях поднимает проблемы разработки принципов и правил обработки большого объема данных, в число которых возможно включение персональных данных, а также соответствия действительности собранных данных и правовых последствий решений, принятых искусственным интеллектом.

Принципы и правила обработки большого объема данных

Необходимо начать с того, что не всегда обработка больших объемов данных включает личные данные. Существует множество примеров неперсональных больших данных, например, данные о погоде, геопространственные данные, астрономические данные, данные, получаемые от датчиков на автомобилях и станках, и др. Кроме того, существует возможность анонимизации собираемых личных данных.

Однако формирование цифрового профиля субъекта напрямую связано с информацией о человеке. В этом случае необходимо определить правовое регулирование не только процедуры получения информированного согласия, но и обеспечения надежности и достоверности источников данных, на основе которых формируется цифровой профиль человека, поскольку он создается именно с целью достоверной идентификации человека и его предпочтений.

Так, с целью развития рынка платежных услуг Банк России создает платформу цифрового профиля, которая «направлена на формирование удобной и безопасной инфраструктуры для обмена данными между государством и бизнесом в режиме онлайн, позволяющей гражданам управлять своими цифровыми данными» (Основные направления развития финансового рынка Российской Федерации на период 2019–2021 годов (разработаны Банком России)).

Создание другой платформы цифрового профиля гражданина предлагает Минкомсвязь России в законопроекте «О внесении изменений в отдельные законодательные акты (в части уточнения процедур идентификации и аутентификации)», данные из которой позволят создать альтернативу идентификации человека по паспорту.

В связи с создаваемыми информационными инфраструктурами цифрового профиля для обеспечения взаимодействия субъектов возникает вопрос о соответствии обработки данных, осуществляемой в инфраструктурах, принципам и правилам обработки персональных данных, предусмотренных в ст. 6 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Данная проблема актуальная во многих государствах, например, Европейская комиссия по эффективности юстиции выработала пять этических принципов при использовании искусственного интеллекта и изложила их в Европейской хартии использования искусственного интеллекта в судебной и правоохранительной деятельности (принята на 31-м пленарном заседании Совета Европы Европейской комиссии по эффективности правосудия, Страсбург, 3–4 декабря 2018 г.) [1]. К этим принципам отнесены: принцип уважения основных прав человека путем обеспечения совместимости дизайна, инструментов и услуг искусственного интеллекта с основными пра-

вами человека; принцип недискриминации, который направлен на предотвращение развития или усиления любой дискриминации между отдельными лицами или группами; принцип качества и безопасности, который определяет, что в отношении обработки судебных решений и данных необходимо использовать сертифицированные источники и данные в безопасной технологической обстановке; принцип прозрачности, беспристрастности и справедливости, который обязывает разработчиков сделать обработку данных и методы доступными и понятными, с возможностью проведения внешнего аудита; принцип «под контролем пользователя», который обязывает исключить предписывающий подход и обеспечить информирование пользователей и контроль их выбора.

Необходимость пересмотра принципов и правил обработки персональных данных в условиях применения технологии больших данных связана с тем, что закрепленные принципы обработки персональных данных были сформулированы для другой технологической среды и небольшого объема данных, реализовать которые в вышеуказанных технологиях невозможно [2]. В связи с этим принимаются новые нормативные правила, учитывающее особенности обработки больших объемов информации.

Например, целью вступившего 25 мая 2018 года в силу закона «Общего регламента о защите данных» (General Data Protection Regulation – GDPR) для всей территории Евросоюза является создание условий субъектам персональных данных (людям ЕС) для обеспечения контроля над данными, которые собираются и обрабатываются в целях создания на их основе цифрового профиля человека.

В Великобритании 23 мая 2018 г. вступил в силу Закон о защите данных (DPA), в котором сформулированы принципы защиты данных, и определены условия осуществления контроля гражданами Великобритании за использованием их личной информации организациями, предприятиями и правительством. Закон о защите данных 2018 г. является реализацией в Великобритании GDPR. В этом законе определены следующие принципы обработки персональных данных, которые должны соблюдать любые лица, обрабатывающие персональные данные и занимающиеся профилированием:

- создания справедливого, законного и прозрачного использования данных;
- использования данных только для явно указанных целей;
- обработки данных адекватными, актуальными технологиями;
- обеспечения возможности уточнения и при необходимости обновления данных;
- хранения данных не дольше необходимого срока;
- обеспечения безопасности обработки данных, включая защиту от незаконной или несанкционированной обработки, доступа, потери, уничтожения или повреждения.

Первый принцип, зафиксированный в Законе о защите данных 2018 года, о справедливости, законности и прозрачности обработки данных субъекта также определен в ст. 5 (1) (a) GDPR. Смысл этого принципа заключается в обеспечении осведомленности человека о проведении обработки его персональной информации и возможности человека оценить последствия обработки его персональной информации, а также контролировать используемые категории данных.

В рамках анализа больших данных особенно сложно реализовать первый принцип. В связи с этим в GDPR для любых лиц, обрабатывающих персональные данные введен принцип персональной ответственности, а также определено требование для всех органов государственной власти и организаций, которые систематически обрабатывают большие объемы данных, в том числе занимаются профилированием назначить сотрудника по защите данных.

В настоящее время в науке ведется дискуссия об «ответственности» алгоритмов в принятии решений, поскольку их роль в данном случае основная [3]. Хотелось бы отметить, что, скорее всего, речь должна идти не об «ответственности» алгоритмов, а об ответственности разработчиков программных технологий, реализующих алгоритмы, обеспечивающие принятие решения и выборку необходимых данных для осуществления действий. Это означает, что с внедрением систем искусственного интеллекта, технологий больших данных и интернета вещей безопасность данных уже не может рассматриваться только с точки зрения соблюдения правовых требований. Необходимо комплексное технико-правовое решение, в котором будут преду-

смотрены требования к жизненному циклу разрабатываемой и реализованной технологии. Так, для обеспечения данного принципа необходимо обязать разработчиков технологий предусмотреть функциональные возможности, обеспечивающие контроль со стороны субъектов персональных данных за аналитикой больших данных и соответствием действительности данных, а также ознакомление с алгоритмами, осуществляющими аналитику. По сути, речь идет о возможности убедиться в том, что алгоритмы не получают дискриминационные, ошибочные или неоправданные результаты, поскольку автоматизированное принятие решения по результатам профилирования человека позволяет предположить ситуацию принятия решения на основании данных, не соответствующих действительности, в результате чего будут приняты неожиданные выводы о человеке с нежелательными для него правовыми последствиями.

В связи с этим в ст. 4 GDPR включены положения, касающиеся последствий профилирования, под которым понимается «любая форма автоматизированной обработки персональных данных, состоящая из использования этих данных для оценки определенных личных аспектов, относящихся к физическому лицу, в частности, для анализа или прогнозирования аспектов, касающихся работы этого физического лица на работе, экономического положения, здоровья, личных предпочтений, интересов, надежности, поведения, местоположения или движения».

В связи с возможностью возникновения подобных ситуаций GDPR требует от компаний не подвергать людей исключительно автоматизированному профилированию и принятию решений. Для этого на контролера данных, осуществляющего профилирование, возложили обязанность использовать математические или статистические процедуры, которые принимают решения совместно с участием человека. Контролер данных должен принять меры также для предотвращения принятия решений, основанных на данных о расе, этническом происхождении, политических убеждениях, религии, членстве в профсоюзе, генетическом статусе, состоянии здоровья или сексуальной ориентации. Хотелось бы обратить внимание на то, что в данной правовой норме речь идет не об исключении обработки специальной категории персональных данных, а об исключении принятия решения на основе таких данных. Это можно объяснить тем, что технология обработки большого объема данных не позволяет исключить эту категорию данных из массива информации, однако это можно сделать на этапе анализа и принятия решений.

Случаи принятия решений сугубо автоматизированными средствами, без участия человека до широкого применения технологии больших данных были редкими. Однако возможности анализа больших данных для развертывания машинного обучения поставили вопросы о прозрачности принятия решений и контроля над ними со стороны субъектов персональных данных.

Описание информированного согласия на проведение обработки

Для обеспечения прав человека при автоматизированном профилировании и принятии решений, влекущих юридически значимые последствия в GDPR, приняты правила защиты физических лиц, зафиксированные в ст. 22. Согласно данной статье, компания может осуществлять принятие исключительно автоматизированных решений только в случаях, если это:

- необходимо для заключения или исполнения договора;
- разрешено законодательством Союза или государства-члена, применимого к контролеру данных;
- выражено в явном согласии человека.

В случае если осуществляемая компанией обработка данных подпадает под положение ст. 22, то компания должна предоставить физическим лицам:

- информацию об обработке их данных;
- простые способы корректировки данных или оспаривания полученного решения.

Для исключения нарушений компаниями требований об обработке персональных данных Европейский совет по защите данных (EDPB), включающий представителей государственных органов по защите данных каждого государства-члена ЕС, с 2018 года разрабатывает руководящие документы, правила, лучшие практики соблюдения требований GDPR [4], в которых определено, что согласие в качестве условия обработки личных данных должно быть конкретным, информационным и «однозначным» и самостоятельно предоставлено субъектом. Кроме того, в каче-

стве лучшей практики предлагаются следующие правила оформления порядка обработки данных, профилирования и автоматизированного индивидуального принятия решений:

– если в процессе анализа информации большими данными компания получила персональные данные косвенным образом, то для обеспечения правовой основы осуществления дальнейшего профилирования и/или автоматического принятия решений и документирования этого в политике безопасности данных компания должна отправить субъекту персональных данных ссылку на заявление о конфиденциальности. Кроме того, компания должна раскрыть процедуру получения доступа к данным, на основе которых был создан цифровой профиль;

– в случае предоставления субъектами своих персональных данных им должна быть предоставлена информация о том, как они могут возражать против любого типа профилирования;

– для создания цифрового профиля необходимо предусмотреть процедуры доступа субъектов персональных данных к личным данным, используемым в профилях, для создания возможности редактирования с целью устранения неточностей данных;

– в случае обработки данных о любых уязвимых группах, включая детей, должны быть предусмотрены дополнительные проверки профилирующих или автоматизированных систем принятия решений.

Компании должны собирать необходимый минимальный объем данных и иметь четкую политику хранения создаваемых профилей и не использовать специальные категории данных в автоматизированных системах принятия решений, если для этого нет законных оснований, но обязаны удалять любые случайно созданные специальные категории данных.

Компании обязаны раскрыть логику автоматизированного процесса принятия решений, профилирования, а также категорий информации и необходимость ее обработки и последствия.

Несмотря на то, что с момента принятия GDPR прошло почти два года, вопросов о применении сформулированных в данном законе положений не уменьшается. В руководящих документах, правилах и лучших практиках особое внимание уделяется действиям, которые субъект персональных данных должен выполнить для того, чтобы можно было считать, что субъект дал свое согласие. Так, для случаев получения согласия в Интернете определено, что процедура оформления согласия на сайте должна моделировать «четкие позитивные действия», например, субъект должен активировать флажок о согласии или выбрать определенные технические параметры. Кроме того, контролер данных должен подтвердить, что согласие было дано, а субъект данных должен иметь возможность отозвать свое согласие.

Модель «уведомления» и «согласия» в контексте технологии больших данных непрактична [5]. Связано это с тем, что характер анализа, осуществляемого с использованием, например, методов искусственного интеллекта как одной из возможных технологий в больших данных, не позволит получить согласие.

Кроме того, традиционная модель получения согласия также подвергается критике [6], поскольку в контексте больших данных необходимо менять подход, заключающийся в оформлении согласия или отказе от его заключения. Анализ, осуществляемый большими данными, требует оформления согласия на каждом этапе получения новых данных и их обработки, поскольку каждый раз меняется контекст получаемых результатов. Таким образом, необходимо использовать модель оформления постепенного согласия, при котором люди могут дать согласие или отозвать его на каждом этапе использования их данных и на всем протяжении их отношений с поставщиком услуг.

Так, Агентство Европейского Союза по сети и информационной безопасности (ENISA) исследовало подобные тенденции и практику реализации подобного оформления согласия и признало, что данный способ является более технически инновационным (D'Acquisito, Giuseppe et al. Конфиденциальность благодаря дизайну больших данных. Обзор конфиденциальности, совершенствование технологий в эпоху анализа больших данных. ENISA, декабрь 2015 г.). Кроме того, данный способ оформления согласия отражен в исследовании, проведенном Королевской инженерной академией [7], которая рассмотрела преимущества аналитики больших данных в нескольких секторах и риски конфи-

денциальности.

Необходимость контроля за порядком обработки персональных данных, источниками данных, логикой алгоритмов принятия решений связана с серьезной проблемой – достоверностью данных и принятием решений на основе этих данных. С одной стороны, контроль субъекта позволяет обеспечить права человека, но с другой стороны, если субъект изменяет собранные данные, то должен быть предусмотрен контроль за действиями самого субъекта, поскольку не исключена ситуация, при которой возможна фальсификация данных самим субъектом. В связи с этим необходимо обеспечить систему двойного контроля субъекта и обработчика данных, а изменения должны вноситься только после проверки документов, подтверждающих выявленное несоответствие действительности.

В Национальной стратегии развития искусственного интеллекта на период до 2030 года, утвержденной Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» в качестве основной определена проблема использования данных, не соответствующих действительности. Для создания правовых условий исключения данной проблемы и обеспечения соответствия действительности обрабатываемых данных к 2030 году «в стране должна быть создана и запущена в работу полноценная система нормативно-правового регулирования в области искусственного интеллекта. … Она должна определить этические нормы, гарантирующие безопасность граждан при использовании машинного разума».

Для решения данной проблемы необходимо не только создать правовое поле для оборота данных, разработать этические нормы, но и ввести ответственность разработчиков программных технологий, может быть определив ее как «ответственность за логику алгоритмов». Ее смысл заключается в том, что пользователи искусственного интеллекта должны получить технологические реализации и гарантии, обеспечивающие прозрачность и объяснимость принятия решений, логики алгоритмов, на основе которых искусственный интеллект функционирует.

Отношения, формируемые посредством таких технологий обработки данных как интернет вещей, и анализа больших данных позволяют заключить, что принятый способ оформления согласия на обработку персональных данных, при котором заранее предусмотрены категории данных, цели и сроки их обработки, больше не является единственным способом правового оформления отношений. Вышеуказанные технологии – данные, используемые для аналитики во многих случаях, создают автоматически, в связи с этим Фонд информационной ответственности (Ведущий глобальный аналитический центр по информационной политике, который успешно работает с регулирующими органами, политиками, лидерами бизнеса, гражданским обществом и другими ключевыми заинтересованными сторонами во всем мире, чтобы помочь в разработке и продвижении законодательства и практики в области защиты данных посредством управления информацией на основе подотчетности) определил четыре типа данных – предоставленные, наблюдаемые, производные и предполагаемые, для каждого из которых предусмотрена своя специфика правового регулирования.

Возрастает важность доверия к информационным технологиям и способам обработки данных, что неизбежно влечет необходимость разработки технологически открытого способа обработки. Автоматически собранные персональные данные и полученные аналитические результаты уже не могут рассматриваться как собственность, принадлежащая компаниям, которыми они могут распоряжаться без согласования с субъектами персональных данных. Важным фактором в возникающих отношениях является подотчетность компаний по осуществляемому анализу больших данных, поскольку решения, сформированные алгоритмами машинного обучения, могут оказаться ошибочными и повлечь юридически значимые последствия.

В Российской Федерации для обеспечения контроля над цифровыми профилями со стороны субъектов персональных данных необходимо разработать регламенты взаимодействия этих субъектов с компаниями, которые занимаются профилированием, и предусмотреть в них условия контроля со стороны субъектов за обрабатываемыми персональными данными и их корректировки в случае несоответствия действительности.

Качество данных является ключевым вопросом в контексте обработки больших данных, и во многом оно зависит от алгоритмов, осуществляющих обработку данных. В связи

с этим в целях обеспечения информационной безопасности необходимо ввести ответственность разработчиков технологий за логику алгоритмов. Защита данных – это уже не только вопрос соблюдения правовых требований, но и комплексное технико-правовое обеспечение. На первый план выходят принципы обеспечения прозрачности и справедливости обработки большого объема данных.

Литература

1. European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment (Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3–4 December 2018). URL: https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c.

2. Zharova A. K., Elin V. The use of Big Data: A Russian perspective of personal data security // Computer Law & Security Review. – 2017. –Vol. 33. no. 4. – P. 482–501.

3. Kirsten M. Ethical Implications and Accountability of Algorithms // Journal of Business Ethics (2019) 160:835–850. URL: https://link.springer.com/content/pdf/10.1007%2Fs10551-018-3921-3.pdf.

4. GDPR: Guidelines, Recommendations, Best Practices. URL: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en.

5. Bayer J. A., Bitiukova N., Bard P., Szakács J., Alemanno A., Uszkiewicz E. Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States // Electronic Journal. – 2019. – January. DOI: 10.2139/ssrn.3409279.

6. Kirsten E. M. Ethical Issues in Big Data Industry, June 2015 MIS Quarterly Executive. URL: https://www.researchgate.net/publication/273772472_Ethical_Issues_in_Big_Data_Indust.

7. Royal Academy of Engineering, November 16, 2015. URL: http://www.raeng.org.uk/publications/reports/connecting-data-driving-productivity0.

Жарова Анна Константиновна – кандидат юридических наук, доцент, старший научный сотрудник, Институт государства и права РАН, г. Москва. E-mail: anna_jarova@mail.ru.

Статья поступила в редакцию 30 апреля 2020 г.

DOI: 10.14529/law200214

LEGAL SUPPORT FOR DIGITAL PROFILING OF HUMAN ACTIVITIES

A. K. Zharova

Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation

The proliferation of systems that analyze large volumes of data and their deep penetration into various areas of human life require the study of emerging legal problems. In this regard, the question is logical – where is the line between the legal consequences created by the analysis of large volumes of data and already become traditional forms of consent and data use. The article explores the problem of legal support of the requirements for informing the subject of personal data when profiling the activities of the subject. To do this, the Russian legislation, the European Union and the United Kingdom are investigated.

Without the development of legal requirements for the processing of large digital data, situations of interference in the private life of a person are possible, the construction of an information model of a person's profile on data that does not correspond to reality, and the adoption of decisions having legally significant consequences on the basis of such models.

The formation of the subject's digital profile is directly related to the information about the person and in this case it is necessary to determine the legal regulation not only regarding the procedure for obtaining informed consent, but also the reliability and reliability of the data sources on the basis of which the person's digital profile is formed, since it is created specifically for reliable identification of a person and his preferences.

Keywords: Internet of things, artificial intelligence, big data, profiling.

Anna Konstantinovna Zharova – Candidate of Sciences (Law), Associate Professor, Senior Researcher, Institute of State and Law of the Russian Academy of Sciences, Moscow, Russian Federation. E-mail: anna_jarova@mail.ru.

Received 30 April 2020.

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Жарова, А. К. Правовое обеспечение цифрового профилирования деятельности человека / А. К. Жарова // Вестник ЮУрГУ. Серия «Право». – 2020. – Т. 20, № 2. – С. 80–87. DOI: 10.14529/law200214.

FOR CITATION

Zharova A. K. Legal support for digital profiling of human activities. *Bulletin of the South Ural State University. Ser. Law*, 2020, vol. 20, no. 2, pp. 80–87. (in Russ.) DOI: 10.14529/law200214.