



МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО НАДЗОРУ В СФЕРЕ СВЯЗИ,
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И МАССОВЫХ КОММУНИКАЦИЙ
(РОСКОМНАДЗОР)**

ЗАМЕСТИТЕЛЬ РУКОВОДИТЕЛЯ

Китайгородский проезд, д. 7, стр. 2, Москва, 109992
тел./факс: (495) 983-33-93; <http://rkn.gov.ru/>

Комитет Совета Федерации
Федерального собрания
Российской Федерации по
экономической политике

OVSkripchenko@senat.gov.ru
IYPylaeva@senat.gov.ru

08.11.2023 № 08ВМ-102249

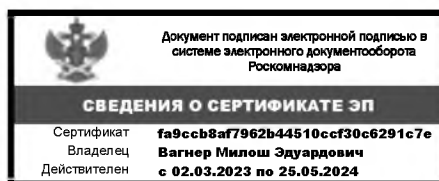
На

О направлении справочно-аналитических
материалов

Рассмотрели письмо Комитета Совета Федерации Федерального Собрания Российской Федерации по экономической политике о проведении «круглого стола» на тему «Обработка и использование больших данных как фактор эффективного развития цифровой экономики: правовое регулирование и актуальные проблемы» и направляем справочно-аналитические материалы по данной теме (прилагаются).

Предложений в итоговый документ не имеется.

Приложение: в 1 экз. на 5 л.



М.Э. Вагнер

Справочно-аналитические материалы к круглому столу по теме «Обработка и использование больших данных как фактор эффективного развития цифровой экономики: правовое регулирование и актуальные проблемы»

Информационные технологии изменили формы и механизмы реальных процессов, которые перетекли в сетевое пространство, где приобретение товаров и услуг, общение с друзьями, взаимодействие с работодателем, государственными органами стали обыденностью. Этому в том числе способствует развитие технических решений, направленных на сбор огромных массивов информации в сети Интернет.

Становится очевидным, что объем данных будет неуклонно расти, равно как и возможности их обработки и использования.

Технологии обработки больших данных и извлечения из них необходимой информации уже существуют и используются в различных отраслях жизнедеятельности.

Так, сбор данных о загруженности транспортной инфраструктуры и миграции населения в рамках крупных городов, как правило, является основой планирования перспективного развития мегаполисов. Учёт количества новорождённых в пределах определённого календарного периода позволяет рассчитать количество дошкольных и общеобразовательных учреждений. «Большие данные» широко используются при оценке качества предоставляемых услуг и могут, в том числе, служить надёжным источником при прогнозировании потребительского спроса.

Если раньше было хорошо известно, что относится к личной информации (имена, адреса номера телефонов, идентификаторы социального страхования и т. д), то и защищать такую информацию можно было с использованием традиционных инструментов. На сегодняшний день реалии таковы, что даже с помощью самой, казалось бы, незначительной и безобидной информации можно установить личность человека. Например, геометка, соотнесенная с профилем в социальной сети, позволяет установить текущее местонахождение. Развитие систем геолокации, появление технологий автоматического распознавания изображений помещают нас в «прозрачный мир», в котором нас легко отследить.

Основная часть создаваемых сегодня платформ «Больших данных» все-таки работает с личной информацией. Некоторые виды данных могут и не быть отнесены явным образом к персональным данным – если рассматриваются фрагментарно, обособленно от других доступных сведений. Но когда такая информация помещена в массив «Больших данных», она может легко стать источником обратной связи с ее носителем.

В контексте «Больших данных» проблема конфиденциальности приобретает новые очертания. Они связаны с недостаточной эффективностью существующих инструментов защиты конфиденциальности, а также с правовыми основаниями и принципом целеполагания. Несоблюдение базовых условий конфиденциальности при обработке информации нарушает права частных лиц, предусмотренных действующим законодательством о неприкосновенности частной жизни. Сборщики данных должны сообщать нам, какую информацию о нас они собирают и с какой целью.

Технические способы защиты неприкосновенности частной жизни в эпоху «Больших данных» сегодня не всегда оказываются достаточно эффективными. Например, это касается анонимизации.

Анонимизация подразумевает удаление из наборов данных всех личных идентификаторов (имя, адрес, номер кредитной карты, дата рождения, номер социального страхования и пр.). Полученные данные, по мнению обработчиков, можно использовать без ущерба для чьей-либо конфиденциальности. Однако, как показали эксперименты ряда иностранных компаний, этот вывод не соответствует действительности.

Отсюда и вытекает высокий уровень значимости должного правового регулирования обезличенных данных.

В понимании Закона «О персональных данных»¹ под обезличиванием понимаются действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Из определения «обезличивания», данного в Законе «О персональных данных», можно вывести понятие обезличенных персональных данных. Это любая информация, которая с помощью совершаемых действий с ней не позволяет без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

В результате обезличивания связь персональных данных с гражданином не разрывается. Анализ нескольких датасетов позволяет быстро профилировать группу людей, в ряде случаев конкретного гражданина и даже восстановить исходные персональные данные, что подтверждает опыт иностранных компаний по анонимизации данных.

Таким образом, обработка и анализ обезличенных данных несет те же риски, что и обработка персональных данных.

¹ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Потенциальные сферы применения обезличенных персональных данных достаточно разнородны.

Несмотря на определенные риски, такие данные являются драйвером, необходимым для социально-экономического планирования и прогнозирования, в том числе в рамках экспериментальных правовых режимов. Очевидна и эффективность использования обезличенных данных в целях развития технологий искусственного интеллекта в Российской Федерации.

В связи с чем, по нашему мнению, в качестве единой площадки для оборота обезличенных персональных данных должна выступать государственная информационная система, в рамках различные пользователи, соответствующие установленным на уровне законодательства требованиям, могут апробировать создаваемые ими технологии искусственного интеллекта.

Дополнительно полагаем необходимым определить методы обезличивания персональных данных, обладающие высокой степенью анонимизации, не позволяющие с использованием современных информационных технологий восстановить персональные данные граждан и определить их принадлежность к физическому лицу.

Должна быть исключена возможность передачи обезличенных персональных данных за пределы указанной государственной информационной системы либо апробации технологий искусственного интеллекта в сторонних информационных системах, поскольку обеспечить контроль за обработкой обезличенных данных на практике невозможно, что создает условия для утечки обезличенных персональных данных.

С начала 2022 года произошло 140 утечек персональных данных. В свободный доступ попали более 600 млн записей с личной информацией граждан. В 2023 году произошло 126 утечек персональных данных, в результате которых в свободный доступ попали 200 млн записей (Приложение №1, Приложение №2). Обезличенные персональные данные, которые содержат важную информацию о поведении граждан, их предпочтениях и иную чувствительную информацию в случае незаконного распространения могут стать объектом преступных посягательств.

Так, постановлением Правительства Российской Федерации от 21.03.2012 № 211 утвержден перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (далее - Перечень).

В соответствии с п.п. 3) п. 1 Перечня одной из мер, направленных, в первую очередь, на минимизацию рисков причинения вреда конкретным гражданам в случае утечки их персональных данных из информационных систем персональных данных, является обезличивание персональных данных согласно требованиям и методам, установленным уполномоченным органом по защите прав субъектов персональных данных.

Роскомнадзором как уполномоченным органом по защите прав субъектов персональных данных в Российской Федерации установлены требования и методы по обезличиванию персональных данных, обрабатываемых в информационных системах персональных данных, в том числе созданных и функционирующих в рамках реализации федеральных целевых программ, которые утверждены приказом Роскомнадзора от 5.09.2013 № 996 (далее - Приказ).

Данные методические рекомендации разработаны с целью оказания помощи операторам, осуществляющим обработку персональных данных и являющимся государственными или муниципальными органами, в выборе предпочтительных вариантов реализации утвержденных требований и методов на практике.

Таким образом, в целях минимизации рисков неправомерного использования обезличенных данных граждан, на наш взгляд, представляется целесообразным выработать комплексное решение, включающее правовые, организационные и технические меры, которые бы учитывали баланс интересов государства и бизнес-сообщества.

