10 июня 2021

Без грифа секретности: избыточный сбор персональных данных запретят

Правительство внесло в Госдуму законопроект, запрещающий отказывать в заключении или исполнении договора потребителю, который не хочет предоставлять свои персональные данные в случаях, когда это не предусмотрено законом. За понуждение будет введена административная ответственность. Специалисты считают, что эти правила нужно распространить и на данные, собираемые сайтами в интернете. Каковы основные источники утечек наших данных, когда можно поделиться личной информацией, а когда лучше воздержаться от этого рассказал наш эксперт Владимир Бобров.

Тайны и обманы

Правительство России внесло в Государственную думу проект федерального закона «О внесении изменения в статью 14.8 Кодекса РФ об административных правонарушениях», предусматривающий запрет на отказ в заключении, изменении, расторжении или исполнении договора потребителю, отказывающемуся предоставлять свои персональные данные в случаях, когда это не оговорено законом, сообщили «Известиям» в комитете по государственному строительству и законодательству.

Говоря проще, предлагаемые поправки должны наложить запрет на принудительный сбор персональных данных россиян. Юридическим языком это формулируется как «запрет на понуждение потребителя под угрозами отказа в осуществлении сделки к предоставлению персональных данных в случаях, когда предоставление таких данных не предусмотрено законодательством РФ и не связано с совершением сделки по реализации товаров, работ, услуг». Кроме того, устанавливается перечень недопустимых условий договора, ущемляющих права покупателей или потребителей услуг.

К недопустимым, к примеру, относятся условия, предоставляющие продавцу право на односторонний отказ от исполнения обязательства или одностороннее изменение его условий — о предмете, цене, сроке и иных согласованных с потребителем условий. «К недопустимым отнесены и условия, которые обусловливают приобретение одних товаров обязательным приобретением других товаров, создают для потребителя иные обременения, в том числе предусматривают обязательное заключение иных договоров, а также предусматривают оказание допуслуг за плату без получения согласия потребителя», — следует из проекта правительственного законопроекта.

— Новый проект закона создан для дополнительной защиты потребителей при сборе и обработке их персональных данных, — разъясняет эксперт Московского финансово-юридического университета (МФЮА) и руководитель адвокатского кабинета «Законъ» Анна Макеева. — Его разработке предшествовало большое количество жалоб со стороны потребителей.

В Роспотребнадзоре рассказали «Известиям» о типичных нарушениях, выявляемых в ходе проверок компаний: «несоответствие содержания письменного согласия субъекта персональных данных на обработку персональных данных требованиям законодательства Российской Федерации, обработка избыточных персональных данных по отношению к заявленным целям их обработки, нарушение права потребителя на свободный доступ к товарам (работам, услугам) путем его ограничения на свободное распоряжение своими персональными данными».

Положения действующего закона «О защите прав потребителей» в нынешней редакции не позволяют в подобных случаях бороться с нарушениями.

Законное «воровство»

Чаще всего персональные данные воруют инсайдеры — люди, имеющие непосредственное отношение к системам, в которых происходит обработка персональных данных и данных в связи с действиями людей, уточняет эксперт по информационной безопасности компании «Акронис Инфозащита» Евгений Родыгин. Иногда информация о внешних «взломах» от потерпевших компаний может оказаться попыткой скрыть такие внутренние инциденты. Часто за утечки выдается вполне осознанная передача данных между заинтересованными лицами в целях развития их бизнеса, подчеркивает эксперт.

80% опрошенных компанией «СёрчИнформ» респондентов сочли «внутренние» (инсайдерские) инциденты более опасными. При этом по данным экспертов, программы для контроля действий сотрудников с

информацией и персональными данными (DLP) стоят только в трети крупных организаций, в малом и среднем бизнесе их число еще меньше.

Начальник отдела информационной безопасности «СёрчИнформ» Алексей Дрозд утверждает, что взлом баз данных — не самая частая причина утечек. Проблема скорее в том, что эти сведения сейчас собирает и хранит едва ли не каждая организация. Попросту говоря, злоумышленникам гораздо проще собирать информацию, которая и так «плохо лежит».

— Первый вариант — парсить данные (собирать на определенных сайтах, с помощью специальных программ), которые пользователи или организации сами выкладывают в интернет, не озаботившись настройками безопасности. Другой вариант для злоумышленников — найти плохо защищенные базы данных. Сплошь и рядом в компаниях забывают о настройках безопасности, в результате базы с персональными данными лежат, по сути, в открытом доступе.

Но новым вызовом в сфере защиты данных является проблема обеспечения сохранности биометрических образцов. А это отдельная категория персональных данных, предупреждают специалисты. Пока же новости про дипфейки появляются всё чаще, а скорость распространения подобных технологий зависит от того, насколько быстро нейросети учатся качественно синтезировать чужую речь и какой объем образца голоса им потребуется.

Дыры и их обитатели

Сейчас в России утечки происходят в четырех секторах обработки персональных данных, рассказывает **руководитель проектов департамента**

ИТ-аутсорсинга компании «КОРУС Консалтинг» Владимир Бобров.

На первом месте — сотовые операторы и телеком-компании. У них большой штат, и доступ к данным имеет огромное количество сотрудников. Основная причина в этом случае — умышленный вывод данных. На втором — банковский сектор. В этой области утечки происходят на этапе сбора данных потенциальных клиентов через сторонние сайты, размещающие рекламу услуг. Также они происходят и через ИТ-специалистов, имеющих доступ к резервным копиям баз данных.

Третье место занимают государственные компании и ресурсы, где, как правило, утечки возможны из-за брешей в системе безопасности сайтов. И последнее — частный бизнес, где причиной утечки становятся ошибки и уязвимости на корпоративных сайтах и в CRM-системах.

Беда еще и в том, что объявления о продаже персональных данных встречаются в Сети всё чаще, подчеркивает руководитель информационной безопасности компании «МойОфис» Александр Буравцов. Злоумышленники активно пытаются получить доступ как к информационным системам государственного сектора, так и к коммерческим базам данных. Так, совсем недавно стало известно об утечке конфиденциальных данных сотен российских компаний из-за небрежного использования программного обеспечения для управления проектами — Trello.

Умолчание — золото

В каких ситуациях потребителю лучше отказываться от предоставления своих данных и почему? Прежде всего в тех случаях, когда покупка товаров или

предоставление услуг не связаны с наличием у продавца персональных данных потребителя, объясняет член Ассоциации юристов России (АЮР) Николай Пивоваров. Например, не нужно предоставлять свои персональные данные при публичной оферте, которая адресована неопределенному кругу лиц. — Не нужно лишний раз предоставлять свои данные при покупке продовольствия в магазине, покупке билета в кино, заказе еды в местах общественного питания — кафе и ресторанах, приобретении одежды, бытовой техники и так далее. Выполнение условий такой сделки купли-продажи и предоставления услуг в форме публичной оферты не зависит от предоставления потребителем его персональных данных — в этом просто нет необходимости, — замечает Пивоваров.

Однако, оговаривается юрист, есть такие услуги и сделки, когда исполнителю необходимо знать ваши персональные данные, так как иначе обязательства не могут быть выполнены, а наличие персональных данных является обязательным условием договора/публичной оферты. Скажем, услуги по доставке продуктов, банковские услуги, услуги страхования и другие, где поставщику услуг/продавцу необходимы паспортные данные, адрес потребителя, его телефонный номер, ИНН, СНИЛС или фотография.

— Вместе с тем не стоит предоставлять свои персональные данные организациям и другим лицам, которые не вызывают у вас доверия, особенно по средствам телефонной связи, — предупреждает специалист.

По мнению президента НП «РУССОФТ» Валентина Макарова, свобода распоряжения личностью своими персональными данными должна быть отражена в Конституции и строго охраняться законом.

Катехизис потребителя

Обязательно уточняйте, действительно ли это обязательно, задавайте вопросы: как и кем данные будут использованы, где они будут храниться, как можно запросить их удаление и т.д. Если не уверены, что вам это нужно — откажитесь от передачи. Передача избыточных данных — обычное дело при регистрации на сайтах и в социальных сетях. Избегайте ввода таких данных, помните, что в большинстве случаев вы не обязаны предоставлять полную информацию о себе.

Так же важно разделять информацию, которую вы можете сменить быстро (адрес электронной почты, номер телефона и т.п.), и ту, что изменить сложно или невозможно (имя, адрес, возраст, пол, номер паспорта), резюмируют специалисты.

Источник: iz.ru