Защита персональных данных – обеспечение конституционных прав и свобод граждан

Protection of personal data – ensuring the constitutional rights and freedoms of citizens

Марданова Г.А.
Младший научный сотрудник лаборатории Правовой информатики и кибернетики юридического факультета МГУ им. М.В. Ломоносова, г. Москва
e-mail: marga3102@yandex.ru

Mardanova G.A.
Junior research scientist of the Law informatics and cybernetics laboratory of the Law Department, Lomonosov Moscow State University, Moscow
e-mail: marga3102@yandex.ru

Аннотация
В 2022 г. наблюдался всплеск утечек персональных данных (ПД) сотрудников, клиентов, пользователей и т.п. в самых различных организациях, учреждениях и ведомствах страны. В статье анализируется эффективность мер, которые предпринимает или планирует предпринять государство для охраны ПД - конституционного права граждан на защиту неприкосновенности частной жизни, личной и семейной тайны. Указано на недостаточность этих мер, в связи с чем даны рекомендации гражданам, которые помогут самостоятельно позаботиться о сохранности своих ПД.
Ключевые слова: персональные данные, информация, утечки данных, интернет-сервисы, безопасность, защита, обработка.

Abstract
2022 the eruption of personal data (PD) breach was detected. Employees, clients, users etc. of different organizations and state institutions were affected. The author has analyzed present and planned PD protection measures provided by State institutions that obtains the Constitutional Right of personal privacy and family secret protection. There was detected the imperfection of the State regulation. Therefore the article contains several recommendations for citizens that may help to protect PD themselves.
Keywords: Personal data, information, data leakage, internet services, security, protection, processing.

Определение понятия «персональные данные» (ПД) дано в ст. 3 одноименного закона №152-ФЗ: «персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)» [1]. Эта информация включает фамилию, имя, отчество (ФИО), число, месяц, год и место рождения, мобильный телефон, e-mail, адрес проживания, фотографию, паспортные данные, сведения о семейном, социальном, имущественном положении, образовании, профессии, доходах и т.д. Строгого списка или перечня ПД нет. Для того чтобы данные можно было считать персональными, они должны содержать ФИО или реквизиты паспорта. Только тогда станет понятно, к кому конкретно относятся телефон, адрес и т.д.

Постановление Правительства РФ от 01.11.2012 №1119 [2] делит ПД на четыре категории: общедоступные, специальные, биометрические и иные ПД. Общедоступные могут быть опубликованы во многих открытых источниках, как, например, ФИО, адрес регистрации, информация о месте работы, номер телефона, e-mail. Специальные обычно находятся в закрытом доступе. Их можно узнать либо лично у человека, либо сделав запрос в соответствующую организацию. К специальным ПД можно отнести расовую и национальную принадлежность, политические, религиозные и философские взгляды, состояние здоровья. Биометрические используют для установления личности человека, например, отпечатки пальцев, группа крови, генетическая информация. Фотография тоже может стать биометрической информацией, если она используется камерой для распознавания лиц. Данные, которые нельзя отнести к первым трём категориям, относятся к категории «иные». Это может быть членство в каком-либо клубе, стаж работы, зарплата и т.п. Иные данные могут часто меняться и фактически являются дополнительной информацией.

Сегодня вопросы, связанные с защитой и обработкой ПД, регулируются законодательством:

- Федеральный закон о персональных данных N 152-ФЗ [1] регулирует процесс обработки, хранения и порядок доступа к ПД. Цель этого закона — обеспечение защиты прав и свобод человека и гражданина при обработке его ПД, в том числе защиты конституционных прав на неприкосновенность частной жизни, личную и семейную тайну [3].
- Закон N 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4]. Статья 15.5 этого закона «Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных» учреждает создании в РФ реестра нарушителей прав субъектов ПД. Туда попадают ресурсы, нарушившие Закон «О персональных данных».
- Закон «О банках и банковской деятельности» [5]. Согласно ст. 26 этого закона к банковской тайне относится информация об операциях, счетах и вкладах клиентов и корреспондентов, при этом кредитная организация гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте, которые также являются его ПД.
- Глава 14 ТК РФ «Защита персональных данных работника» [6].
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [2].
- Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» [7].
- Статья 13.11 КоАП РФ, где прописана ответственность за нарушения правил работы с ПД [8].
- Статья 137 УК РФ «Нарушение неприкосновенности частной жизни» [9], по которой тоже может наступить ответственность за нарушение правил обращения с ПД. При этом необходимо доказать, что нарушитель имел прямой или косвенный умысел причинить вред человеку.

Однако рекордное увеличение фактов утечек ПД в 2022 г. показало недостаточную эффективность существующего законодательства в их защите. Практика применения этого законодательства фактически свелась к ритуальному подписанию согласий на обработку данных и пользовательских соглашений, которые мало кто читает и никто не придерживается. При этом субъекты ПД

фактически никогда не получали адекватную компенсацию за разглашение их личной информации. Изменения в законодательстве призваны улучшить ситуацию.

С 1 сентября 2022 г. вступил в силу Федеральный закон от 14.07.2022 № 266-ФЗ (за исключением отдельных положений) [10], которым вносятся изменения в нормативно-правовые акты, регулирующие обработку ПД. Отмечу основные новации:

- Операторам прямо запрещено отказывать гражданам в обслуживании при несогласии последних предоставить свои персональные данные в случаях, когда это необязательно. Раз невозможно полностью исключить вероятность того, что данные окажутся в открытом доступе, следует минимизировать количество предоставляемой информации.
- Ограничена обработка биометрических персональных данных несовершеннолетних.
- Иностранные лица обязаны соблюдать положение Закона № 152-ФЗ при обработке персональных данных, т.е. российское законодательство о персональных данных применяется за пределами страны.
- Персональные данные из ЕГРН предоставляются третьим лицам только с согласия субъекта ПД. Для этого в ЕГРН будут вносить соответствующую запись. За удостоверением факта наличия сведений в ЕГРН о правообладателе недвижимости нужно обращаться к нотариусу. Это изменение способствует сохранности данных ЕГРН, но у него есть и оборотная сторона: «риелторы считают, что если данные из ЕГРН будут закрыты для третьих лиц, то проверить подлинность документов на жилье обычным гражданам станет значительно сложнее. Таким образом, аферистам станет проще обмануть доверчивых граждан, выдав себя за собственника, получив задаток и исчезнув с деньгами…. Сегодня все участники сделок купли-продажи жилья полагаются на данные этого реестра. Но после вступления в силу поправок опираться, по сути, будет не на что» [11].
- Новые правила трансграничной передачи ПД начинают действовать с 1 марта 2023 г. Операторы будут обязаны направлять уведомление в Роскомнадзор о намерении осуществлять трансграничную передачу ПД. При этом вводится два режима уведомлений в зависимости от того, обеспечивает иностранное государство адекватную защиту прав субъектов ПД или нет.
- Сокращены сроки на исполнение запросов Роскомнадзора с 30 до 10 рабочих дней с даты их получения.
- Операторы персональных данных должны проводить оценку вреда, который может быть причинен субъектам ПД нарушением Закона о персональных данных.

Для выполнения последнего пункта 28 ноября 2022 г. в Минюсте России был зарегистрирован Приказ Роскомнадзора от 27.10.2022 г. № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» [12]. Приказ вступает в силу с 1 марта 2023 г. и действует до 1 марта 2029 г.

Согласно этому приказу, оператор определяет одну из степеней вреда, который может быть причинен субъекту ПД – высокую, например, при обработке биометрической и специальной категории ПД; среднюю, например, продвижение товаров с использованием баз ПД других операторов; либо низкую, например, ведение общедоступных источников ПД. Результаты оценки вреда оформляются актом. Указанные степени показывают потенциальный вред, который может быть причинен субъекту ПД, и актуальность угроз безопасности.

Познакомившись с действующим законодательством в области ПД и внесенными в него изменениями, постараемся понять, насколько они помогут улучшить решение вопроса о защите ПД, который стал крайне острым. В последние годы идет активная цифровизация общества и расширение дистанционного взаимодействия. «Пандемия выступила в роли катализатора процесса, выяснилось, что такое взаимодействие удобно, доступно и менее затратно. Институт дистанционного взаимодействия продолжает развиваться» [13]. Как следствие, вырос риск утечки и мошеннического использования добытой незаконным путем информации. «Так, широкое распространение получили интернет-сервисы, занимающиеся противоправным оборотом ПД, где можно приобрести информацию в отношении большинства российских граждан из различных баз данных (адреса, недвижимость, паспорта, сведения об авиа- и железнодорожных перелетах и т.п.)» [13]. По заявлению Роскомнадзора: «С начала военной операции резко увеличилось количество утечек персональных данных – более 140 случаев, в сеть попали около 600 миллионов записей о гражданах» [14]. Более внушительную цифру указывает «Лаборатория Касперского» - 1,5 миллиарда записей в 2022 г. попали в открытый доступ [15]. По утверждению российского сервиса DLBI (Data Leakage & Breach Intelligence), который анализирует сливы, хакерские атаки в 2022 г. впервые стали основным источником утечек. В так называемые кибервойска вовлечено большое количество жителей Украины и других стран.

Наиболее громкими являются случаи утечек информации о клиентах и сотрудниках «Яндекс.Еды», Delivery Club, Wildberries, СДЭК, «Билайна», «Вкусвилла», Whoosh, «Ситимобила», «Гемотеста». Хотя Роскомнадзор блокировал сайты, где выкладывалась слитая информация, она оставалась доступной в сети, а коммерческие компании в итоге оштрафовали на незначительные суммы - от 60 до 100 тыс. руб.

Поправки законодательства могут помочь ограничить сбор ПД и облегчить устранение последствий утечек, но не направлены на ликвидацию причин и предотвращение таких ситуаций. «Как показывает практика, чаще всего "сливы" случаются из-за действий конкретных сотрудников компании, которые хотят продать данные "на стороне". Кроме того, все чаще случаются кибератаки на инфраструктуру операторов. Закон может только усилить ответственность за неправомерную обработку данных, но не предотвратить утечки… Способы, которые действительно работают - ужесточение технических требований и наказаний» [16].

Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифры) выступает за то, чтобы компании активнее инвестировали в системы информбезопасности. Для этого предлагается проводить ежегодный добровольный аудит защищенности данных с привлечением, например, аккредитованных государством компаний, занимающихся информационной безопасностью: Positive Technologies, «Лаборатория Касперского» или Group-IB.

Подтолкнуть компании к модернизации своих систем безопасности могут и увеличение штрафов за утечки. Ещё в конце мая 2022 года Минцифры согласовало законопроект о штрафах для бизнеса за утечки ПД клиентов. Наказание предполагало наложение штрафа, размер которого связан с размером годового оборота компании, так называемый оборотный штраф. При попытке предпринимателей скрыть инцидент, размер штрафа увеличивался. Но только в конце 2022 г. этой инициативе, наконец, дали «зеленый свет». По сообщению «Интерфакса», 7 декабря 2022 г. на заседании Совета по развитию гражданского общества и правам человека, президент Владимир Путин поручил ужесточить наказание за слитую информацию. Компании, допустившие утечки ПД, будут

выплачивать оборотные штрафы. Предложения должны быть готовы до 1 июля 2023 г. В нынешнем законопроекте Минцифры сумма штрафов варьируется от 5 млн до 500 млн руб. и затрагивает только бизнес. Ответственность госорганов в случае утечек с их стороны не указана.

Время покажет, как изменения в законодательстве отразятся на защите ПД. Введение оборотных штрафов должно заставить компании усилить защиту ПД клиентов, сотрудников, пользователей. Создание прозрачной правовой и нормативно-технической базы и, как следствие, формирование культуры защиты ПД, должно привести к улучшению ситуации в этой области.

Однако нормативное регулирование никак не затронуло вторую сторону противоправного процесса – тех, кто незаконно пользуется слитыми ПД. Можно убеждать граждан для сохранности имущества и денег возводить высокие заборы, пользоваться хитрыми замками и дорогими сейфами, но, если вор не будет наказан, воровство будет продолжаться. В нашем случае идет воровство ПД. Поэтому необходимо ужесточить наказание для тех, кто продает базы данных, кто взламывает системы и крадет ПД, а также тех, кто незаконно ими пользуется. Причем наказание должно быть таким, чтобы никому не захотелось с этим связываться. «Наказание за утечку персональных данных надо значительно усилить, считают в Совете по правам человека при президенте России. Подготовку инициатив уже начали, в первых числах февраля их обсудят с законодателями, профильными ведомствами и бизнесом, выяснили «Известия». Важно, чтобы помимо штрафов реальные участники похищений и перепродажи таких сведений получали реальные тюремные сроки, считают общественники. Уголовное наказание должно распространяться и на тех, кто допустил такую халатность, а также покупателей данных» [17]. В Госдуме заверили, что законодатели готовы прислушаться к инициативе СПЧ.

А тем временем утечки данных продолжаются. 13 января 2023 г. телеграм-канал «Утечки информации» сообщил, что в открытом доступе появились 3,5 млн пользователей почты Mail.ru. Среди опубликованных данных — адреса почты, ники, имена и фамилии, а также телефоны пользователей.

Приведу примеры возможного использования ПД, которые легко найти в Интернете. «Популярен» в среде злоумышленников шантаж: через социальные сети они способны вымогать деньги в обмен на то, что не будут использовать Ваши ПД. Был случай, когда не поддавшегося на угрозы молодого человека широкой рассылкой по всем соцсетям объявили преступником, которого разыскивает полиция. Или оформление кредита на Ваше имя в банке. Помимо того, что Вы будете должны банку, Ваша кредитная история будет испорчена при просрочке платежа. Перечень можно продолжать. Обращение в полицию помогает решить вопрос с мошенниками, но это стоит большого количества времени и нервов.

Исходя из сложившейся ситуации, нельзя рассчитывать только на государство, в настоящее время сами граждане тоже должны заботиться о безопасности своих ПД. К сожалению, россияне к этому пока не готовы. В феврале 2022 г. компания-разработчик антивирусных решений ESET поделилась итогами исследования, цель которого - определить, как жители страны относятся к сбору и передаче ПД на сайтах и в приложениях [18]. Оказалось, что 40% участников опроса отрицательно относятся к сбору ПД, потому что не верят в конфиденциальность этого процесса, 38% респондентов выразили нейтралитет. Но главное, 92% участников опроса не беспокоит, если данные о них передаются третьим лицам! Они не стараются покинуть сайт или приложение, в пользовательском соглашении которого обозначена такая функция, это соглашение подавляющее большинство (94%) или не дочитывают до конца, или совсем не читают.

Большинство наших граждан остаются в полном бездействии. На данном этапе надо совместно с государством заботиться о сохранности своих ПД. Приведу несколько полезных рекомендаций, которые легко выполнимы:

- В онлайн-сервисах необязательно указывать реальные ПД. Для интернет-магазинов, служб доставки и т.п. достаточно действующего номера телефона.
- Желательно не предоставлять сканы, фотографии или копии паспорта и других документов, а если без этого не обойтись, можно сделать на нем надпись о том, что он предоставлен для такой-то организации. Например, скан для каршеринга. Во-первых, в случае утечки ПД будет понятно откуда они утекли; во-вторых, взять кредит с таким сканом, где указано для кого он предназначен, не получится. Мошенники скорее выберут другую кандидатуру.
- Следует завести отдельную почту для регистрации в интернет-сервисах и программах лояльности. Как ПД она будет для Вас не важна, да и ненужная реклама будет «сыпаться» именно туда.

Согласно ст. 24 Конституции Российской Федерации: «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются» [3], значит защита наших ПД – это забота государства. Хочется надеяться, что законодатели не остановятся и продолжат совершенствование нормативного регулирования вопроса защиты ПД.

Литература

1. Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"// "Российская газета" от 29 июля 2006 г. N 165. Система ГАРАНТ.
2. Постановление Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"// "Российская газета" от 7 ноября 2012 г. N 256. Система ГАРАНТ.
3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Система ГАРАНТ.
4. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// "Российская газета" от 29 июля 2006 г. N 165. Система ГАРАНТ.
5. Федеральный закон от 2 декабря 1990 г. N 395-I "О банках и банковской деятельности" // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. N 27 ст. 357. Система ГАРАНТ.
6. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. N 197-ФЗ // "Российская газета" от 31 декабря 2001 г. N 256. Система ГАРАНТ.
7. Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» // «Российская газета» от 24 сентября 2008 г. N 200. Система ГАРАНТ.
8. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ // Российская газета от 31 декабря 2001 г. N 256. Система ГАРАНТ.
9. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954. Система ГАРАНТ.
10. Федеральный закон от 14 июля 2022 г. N 266-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", отдельные законодательные акты

Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона "О банках и банковской деятельности" // Российская газета, 20 июля 2022 г. N 156-157. Система ГАРАНТ.
11. Данилов С. Защита персональных данных: новые требования и обязанности фирм / С. Данилов // журнал «Практическая бухгалтерия». – 2022. - № 10.- С. 69-75.
12. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. N 178 "Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона "О персональных данных" // официальный интернет-портал правовой информации (pravo.gov.ru), 29 ноября 2022 г. , N 0001202211290004.
13. Королева Я.Ю. Изменения в законодательстве, касающиеся персональных данных / Я.Ю. Королева// журнал «Руководитель бюджетной организации». – 2022. - № 8. - С. 42-49.
14. LENTA.RU [Электронный ресурс] // Режим доступа на 16.01.2023: https://m.lenta.ru/news/2022/12/16/leaks/
15. RG.RU [Электронный ресурс] // Режим доступа на 16.01.2023: https://rg.ru/2022/12/08/bolee-15-mlrd-zapisej-s-personalnymi-dannymi-popali-v-set-v-2022-godu.html
16. Новые правила защиты персональных данных сильно усложнят работу компаний // журнал «Практическая бухгалтерия». – 2022. - № 6. - С. 27-31.
17. Набаткина К. Сливы дорожают: в СПЧ предлагают сажать за утечку личных данных. 20.01.2023 [Электронный ресурс]// Режим доступа на 20.01.23 https://iz.ru/1457311/kseniia-nabatkina/slivy-dorozhaiut-v-spch-predlagaet-sazhat-za-utechku-lichnykh-dannykh
18. Портал TADVISER.RU. Статья «Защита персональных данных в России» [Электронный ресурс] // Режим доступа на 16.01.2023: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%97%D0%B0%D1%89%D0%B8%D1%82%D0%B0_%D0%BF%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%8B%D1%85_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8#.D0.98.D1.81.D1.81.D0.BB.D0.B5.D0.B4.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D1.8F