DOI: 10.17747/2311-7184-2021-11-314-317

Защита и конфиденциальность данных граждан на платформе цифрового профиля гражданина

В.В. Ветрова, студент, Финансовый университет при Правительстве РФ (Москва, Россия)
vika.vetrova.2001@mail.ru
Научный руководитель: О.Е. Устинова, к.э.н., доцент, Финансовый университет при Правительстве РФ (Москва, Россия)
oeustinova@fa.ru

Аннотация. В статье рассмотрены вопросы конфиденциальности цифровых данных граждан и безопасности их хранения в цифровом профиле гражданина. Ввиду масштабности этой системы, а также ценности хранимой информации возникает большой риск утечки или незаконного получения конфиденциальных данных, которые могли бы представлять коммерческую ценность для многих субъектов, чем обусловлена актуальность вопроса.

Ключевые слова: цифровой профиль гражданина, безопасность, конфиденциальность, цифровые данные, защита персональных данных.

Protection and confidentiality of citizens' data in the digital citizen profile platform

V.V. Vetrova, student, Financial University under the Government of the Russian Federation (Moscow, Russia)
vika.vetrova.2001@mail.ru
Academic supervisor: O.E. Ustinova, cand. sci. (econ.), associate professor, Financial University under the Government of the Russian Federation (Moscow, Russia)
oeustinova@fa.ru

Abstract. The article deals with the issue of confidentiality of citizens' digital data and the security of their storage on the platform of a citizen's Digital Profile. Due to the scale of this system, as well as the value of the stored information, there is a high risk of leakage or illegal receipt of confidential data that could be of commercial value to many entities, which is why this issue is relevant.

Keywords: digital citizen profile, security, confidentiality, digital data, personal data protection.

Введение

Важнейшим аспектом при создании любой персональной информационной системы является обеспечение ее безопасности, определяющей уровень доверия владельцев данных. Одной из таких систем выступает цифровой профиль гражданина. Несмотря на то что предоставление цифровой идентификации гражданину имеет большое количество преимуществ, к примеру является эффективным инструментом облегчения и оптимизации доступа к необходимым данным для государственных органов, подключения каждого человека к государственным и частным сервисам, укрепления и ускорения социальной и финансовой интеграции, вместе с тем возникают риски, связанные со всевозможными утечками и извлечением коммерческой выгоды из персональной информации. В этой связи обозначена проблема определения уровня безопасности хранения данных в системе цифрового профиля гражданина.

Литературный обзор

Проблема безопасности хранения персональных данных в сети интернет затронута в работах разных авторов. В исследовании В. Солдатовой [6] рассмотрена правовая основа регулирования защиты данных и ответственности за нарушение в этой сфере. В статье А. Бадьиной и М. Орешиной [1] затрагиваются общие вопросы организации системы цифрового профиля гражданина и особенности предоставления доступа к данным. Информационная статья RBK рассматривает риски утечки данных, отмеченных на государственном уровне [4], опыт Google [2]. В статье MKRU «обозначены риски создания цифрового профиля каждого россиянина» [3], исследование NTV посвящено тонкостям организации цифровой платформы [9].

Законодательство о доступе к информации и связанные с ним законы о конфиденциальности появились отчасти потому, что граждане и правительства озабочены тем, чтобы защитить свои права и задокументировать свои обязанности в эпоху постоянных изменений в процессе общения и сбора данных [5].

Защита персонализированных данных в нашей стране регулируется законодательными актами различных уровней. Основополагающим является Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [8], главной целью которого является обеспечение защиты прав и свобод граждан при обработке персональных данных, в том числе прав на неприкосновенность частной жизни и личной тайны. Нормы этого закона прямо коррелируют со статьей 152.2 Гражданского кодекса РФ об охране частной жизни гражданина.

Одним из основных регулирующих механизмов этого акта законодательства является право на обезличивание информации о конкретном лице. Под обезличиванием понимается вызванная определенными действиями ограниченность данных, в результате которой невозможно точное определение принадлежности информации конкретному субъекту без использования дополнительных источников.

Отдельно стоит отметить и регламентированное в 2015 году законом №264-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»» [7], право на забвение в сфере персональных данных в сети. Согласно этому акту операторы поисковых систем интернета обязаны ограничивать доступ к ссылкам на информацию о пользователях, обратившихся с такими требованиями.

Сегодня эти нормативно-правовые акты являются базисом правового регулирования сбора, обработки и использования персональных данных.

Нельзя не отметить тот факт, что конфиденциальность информации в системе цифрового профиля – это на сегодняшний день самый обсуждаемый и спорный вопрос, который поднимается не только среди потенциальных пользователей сервиса, но и на межведомственном уровне. Опасения у граждан вызывают возможные утечки информации, которые могут быть связаны в первую очередь с большим объемом сведений, хранящихся в базе данных, их детализацией и, соответственно, большой ценностью для коммерческих организаций и иных заинтересованных лиц [6].

Противники этой законодательной инициативы считают, что сбор такого количества сведений выступает как прямое нарушение личной свободы граждан, что, в свою очередь, может отрицательно повлиять на состояние общественных отношений в целом. Недоверие граждан вызывает и возможность в перспективе использования цифрового профиля не только финансовыми учреждениями для скоринга, но и различными коммерческими организациями для навязывания своих услуг (например, доступ к медицинским данным гражданина может активно использоваться фармацевтическими компаниями для продвижения своих товаров).

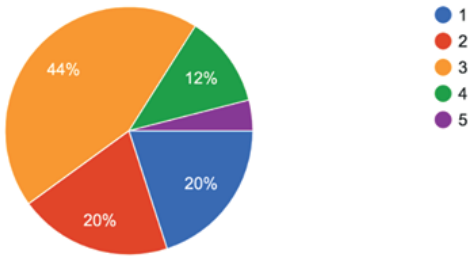
Методы

Методы теоретического исследования интегрированы эмпирическими методами исследования. В качестве основного метода в работе использован качественный подход, позволивший исследовать критерии и факторы, влияющие на обеспечение конфиденциальности сведений о физических лицах, выбор сделан в пользу анкетирования российских граждан. Систематизация и обработка полученных ответов респондентов осуществлялись в соответствии с требованиями обеспечения надежности социологической информации путем обобщения информации в сводной таблице и дальнейшего выделения особенностей. Целью работы является изучение обеспечения конфиденциальности личной информации граждан, хранящейся в сети интернет. Задачами исследования выступают идентификация рисков, определение степени защищенности данных и наступления ответственности за нарушения в этой сфере, изучение зарубежного опыта, а также разработка рекомендаций по обеспечению безопасности персональных данных.

Результаты

Согласно результатам социологического опроса, проведенного при участии 90 человек различных возрастных категорий (от 19 до 60 лет и старше), более 23% из них выразили полное недоверие к защите и безопасности цифровых сведений о гражданине в данной системе по пятибальной шкале. При этом подавляющее большинство (38,2%) все же считают данную систему относительно безопасной (рис. 1).

Рис. 1. Оценка безопасности и защиты цифровых сведений о гражданине



Источник: отчет о научно-исследовательской работе ВТСК «Цифровой профиль гражданина: сущность, содержание, варианты изготовления, оформления, учета и контроля»

Претензии к законопроекту были выделены Федеральной службой безопасности РФ и депутатами Государственной Думы РФ, где основными вопросами стали:

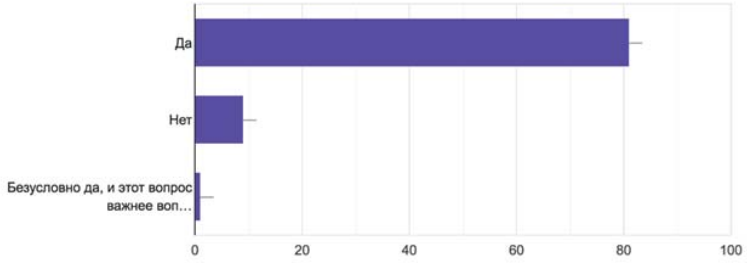
1) отсутствие собственника цифрового профиля, который имеет право распоряжаться данными;
2) отсутствие законодательно закрепленных санкций со стороны уполномоченных органов за нарушение конфиденциальности или попытки незаконного изъятия данных;
3) необратимость сделок, совершенных без ведома владельца профиля [4].

Опасения представителей государственных органов не беспочвенны: ведь только за последний год количество попыток незаконного получения конфиденциальных данных выросло на 46% (в прошлом году зафиксировано 395 случаев утечек со 172 млн записей персональной информации), при этом количество утерянных

записей увеличилось в 6 раз [3]. Многие эксперты в сфере интернет-безопасности утверждают, что подобная система, позволяющая получить доступ к целому ряду данных через единое окно, может быть уязвима для атак и, следовательно, существенно влияет на статистику в худшую сторону.

Результаты социологического опроса также показывают, что именно такой вариант доступа к хранящейся информации вызывает наибольшие сомнения ее владельцев (рис. 2). Около 80% респондентов высказали недоверие к системе единого окна.

Рис. 2. Уязвимость системы доступа к персональным данным через одно окно для действий мошенников



Источник: отчет о научно-исследовательской работе ВТСК «Цифровой профиль гражданина: сущность, содержание, варианты изготовления, оформления, учета и контроля»

Таким образом, возникает вопрос: насколько безопасен сервис цифрового профиля граждан в Российской Федерации с точки зрения конфиденциальности данных и насколько качественно обеспечивается их сохранность в нем? Представители Центрального банка РФ утверждают, что поводов для опасений граждан на сегодняшний день нет: ведь именно из соображений безопасности было решено отказаться от изначальной инициативы уменьшать затраты на инфраструктуру проекта за счет коммерческих средств. Как утверждает первый заместитель председателя ЦБ О. Скоробогатова, цифровая платформа оформлена с учетом необходимых мер по защите данных на базе электронного правительства, инфраструктура которого принадлежит исключительно государству [3].

Ярким примером, подтверждающим данную информацию, является отказ Центробанка от сотрудничества с Ростелекомом, который предлагал инвестировать в проект более 3 млрд руб. Эти вложения могли полностью покрыть все расходы по разработке и созданию самой системы, однако чтобы избежать извлечения выгоды из проекта коммерческими организациями государство занялось созданием системы за свой счет [9]. В ЦБ также заявили, что в рамках собственного профиля системы россияне будут сами контролировать и определять, кому и какую информацию о себе они хотят передать.

Во многих развитых странах критика безопасности является также достаточно распространенным явлением. К примеру, Facebook и Google до сих пор критикуют за централизацию данных, собранных о пользователях, что чревато повышенными рисками утечек больших массивов информации, а также использованием их в коммерческих целях. При этом сами компании для предотвращения спорных вопросов обеспечили пользователей сервисом уведомлений о любых возможных действиях обработки информации [2]. Во многих европейских странах вопросу конфиденциальности и безопасности данных уделяют ключевое внимание, так как многие нарушения, когда-либо имевшие место, имели, как правило, серьезные последствия для общества. Именно поэтому было разработано общеевропейское положение о конфиденциальности – General Data Protection Regulation, основные принципы которого:

- обработка данных созданной базы должна производиться по строго ограниченной цели, заявленной при организации сбора информации;
- объем личных данных, необходимых для сбора по определенной цели, не должен превышать изначально заявленный;
- срок хранения личных данных должен быть ограничен тем, который необходим для достижения заявленной цели.

Одним из наиболее значимых вопросов этого положения стало право на распоряжение своими данными, в том числе на их перенос и передачу другому лицу или организации в его формате запроса.

Нельзя не упомянуть и то, что европейское общество в принципе довольно неоднозначно принимает идею создания единых цифровых платформ и сосредоточения огромного массива конфиденциальной информации о гражданах в одном месте [1].

Учитывая разные подходы и мнения к созданию цифрового профиля гражданина, а также результаты проведенного исследования, включающие проблемы обеспечения безопасности и сохранности персональных данных, целесообразно предусмотреть:

- возможность запроса на согласие пользователя в отношении доступа к его персональной информации;
- получение данных из регистров, хранящихся в цифровом профиле, информационными системами участников проекта;
- уведомление участников цифрового профиля об изменениях в регистрах, хранящихся в нем.

Для выполнения определенных действий с данными пользователя в различных целях организации, имеющие к ним доступ, должны получить от пользователя согласие в течение запрашиваемого периода [10]. Кроме того, россияне смогут в любой момент увидеть реестр своих согласий на обработку персональных данных организациями и отозвать те из них, которые считают нецелесообразными. Однако необходимо учитывать тот факт, что законом предусмотрены случаи, когда получение данных из реестра сможет осуществляться и без согласия их владельца.

Создание цифрового профиля не должно осуществляться без получения согласия гражданина, которое впоследствии он сам вправе отозвать. Для соблюдения конфиденциальности в таком случае сервис и банк-получатель обязаны удалить все данные лица и прекратить дальнейшую всевозможную их обработку. При этом гражданину направляется гарантированное уведомление от финансовой организации о прекращении использования его персональных данных или сроке, когда оно произойдет.

Высокий уровень защищенности при получении услуг обеспечит также дальнейшее развитие на базе инфраструктуры цифрового профиля инструментов облачных квалифицированных подписей.

На основе этого документа можно выделить некоторые рекомендации, которые могли бы существенно повысить конфиденциальность и безопасность системы цифрового профиля гражданина:

- Обработку информации, размещенной в цифровом профиле, целесообразно предоставить пользователям портала, в частности государственным организациям, строго в пределах целей обращения к ней и в объеме, являющимся достаточным для их осуществления.
- Ввиду недостаточно развитой правовой базы обеспечения безопасности цифровой информации, а также отсутствия полной регламентации санкций со стороны государства за незаконные действия в этой сфере необходимо разработать меры пресечения утечек персональных данных в системе цифровых профилей граждан.
- Следует предусмотреть внедрение более надежных способов защиты персональной информации посредством полного перехода системы на индивидуальные цифровые подписи граждан.

Таким образом, в связи с тем, что к вопросу защиты и конфиденциальности платформы цифрового профиля гражданина на современном этапе предъявляется достаточно большое количество требований, он всесторонне регламентируется со стороны государства и обеспечивается его законодательной и исполнительной силой. Благодаря новейшим технологиям защиты персональной информации пользователи сервиса могут без опасений размещать информацию о себе, а также в полной мере использовать все его преимущества.

Использованные источники

1. *Бадьина А.В., Орешина М.Н.* Основные направления развития концепции цифрового профиля. Зарубежный опыт и перспективы развития // Вестник ГУУ. 2020. № 7. URL: https://cyberleninka.ru/article/n/osnovnye-napravleniya-razvitiya-kontseptsii-tsifrovogo-profilya-zarubezhnyy-opyt-i-perspektivy-razvitiya.
2. Google обвинили в незаконном сборе данных и пригрозили штрафом $ 5 млрд. URL: https://www.rbc.ru/technology_and_media/03/06/2020/5ed790e49a7947813766c80ehttps://www.rbc.ru/technology_and_media/03/06/2020/5ed790e49a7947813766c80e.
3. *Деготькова И.* Обозначены риски создания цифрового профиля каждого россиянина. URL: https://www.mk.ru/economics/2020/09/25/oboznacheny-riski-sozdaniya-cifrovogo-profilya-kazhdogo-rossiyanina.html.
4. *Посыпкина А.* В Госдуме указали на риск утечки данных из-за проекта о цифровом профиле. URL: https://www.rbc.ru/technology_and_media/13/01/2020/5e1c69949a79475870438a94.
5. *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «больших данных» (BigData) // Право. Журнал ВШЭ. 2015. № 1. С. 43–66.
6. *Солдатова В.И.* Защита персональных данных в условиях применения цифровых технологий // Lex Russica. 2020. № 2(159). URL: https://cyberleninka.ru/article/n/zaschita-personalnyh-dannyh-v-usloviyah-primeneniya-tsifrovyh-tehnologiy.
7. Федеральный закон «О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации"» // Собрание законодательства Российской Федерации. 29.07.2017 № 276-ФЗ (посл. ред.).
8. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (посл. ред.) // Собрание законодательства Российской Федерации.
9. Цифровой профиль россиянина: ответы на главные вопросы. URL: https://www.ntv.ru/cards/2941/.
10. *Шувалова М.* Минкомсвязь России: закон о цифровом профиле граждан и организаций должен быть принят в этом году. 2019. 28 марта. URL: http://ivo.garant.ru/#/document/77526217.