

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ГРАЖДАН В ЦИФРОВОМ ПРОФИЛЕ¹

Активное развитие цифрового профилирования и использование возможностей цифровых профилей гражданина различными коммерческими организациями ставит задачу по обеспечению информационной безопасности данных процессов. Информационные риски и угрозы сегодня отчетливо проявляются как в части несанкционированного сбора информации о гражданах из цифровых профилей, так и в части незаконного их использования, в том числе для мошеннических целей. Государством ставится задача по защите прав граждан в связи с функционированием цифровых профилей, в первую очередь, защите их персональных данных и иной информации, составляющей личную и семейную тайну.

В статье автором анализируются проблемы, складывающиеся в процессы функционирования системы «Цифровой профиль», а также предлагается ряд мер по обеспечению защиты персональных данных граждан в цифровом профиле.

Ключевые слова: информационная безопасность, правовая охрана, персональные данные, распространение персональных данных в сети Интернет, цифровой профиль.

Minbaleev A. V.

PROBLEMS AND PROSPECTS OF ENSURING THE PROTECTION OF PERSONAL DATA OF CITIZENS IN THE DIGITAL PROFILE

The active development of digital profiling and the use of the capabilities of digital citizen profiles by various commercial organizations poses the task of ensuring the information security of these processes. Information risks and threats are clearly manifested today both in terms of unauthorized collection of information about citizens from digital profiles, and in terms of

¹ Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации (грант МД-2209.2020.6) «Развитие системы правовых средств обеспечения кибербезопасности в Российской Федерации».

their illegal use, including for fraudulent purposes. The State sets the task of protecting the rights of citizens in connection with the functioning of digital profiles, first of all, the protection of their personal data and other information constituting personal and family secrets.

In the article, the author analyzes the problems developing in the processes of functioning of the "Digital Profile" system, and also proposes a number of measures to ensure the protection of personal data of citizens in the digital profile.

Keywords: *information security, legal protection, personal data, dissemination of personal data on the Internet, digital profile.*

В связи с успешным проведением эксперимента по внедрению и использованию системы «Цифровой профиль» можно однозначно говорить о его переходе в следующем году в режим штатного функционирования и использования государством. Однако создание цифрового профиля, с одной стороны, повышает качество жизни и доступность сферы публичного управления для гражданина, с другой стороны, существенно обостряет риски информационной безопасности, ущерб от которых может быть невосполнимым [1].

Создание единого цифрового профиля без должной его защиты и внесения соответствующих изменений в информационное, гражданское, административное и уголовное законодательство, приведет к увеличению числа преступлений в данной области, поскольку незаконное получение сведений из цифрового профиля будет приобретать еще больший интерес, в связи с большим объемом сведений, содержащихся в нем. Функционирование цифровых профилей предусматривает добровольный характер, в том числе, отказ от сбора и обработки персональных данных. Однако у этого решения будут юридически значимые последствия в связи с невозможностью совершения ряда юридически значимых действий после отзыва согласия на обработку персональных данных, фактически речь идет о «добровольном» ограничении правового статуса. Все эти и другие проблемы, к сожалению, сегодня не решены, что вызывает серьезную обеспокоенность.

Анализ современного состояния правового регулирования цифрового профиля в России позволяет систематизировать и выделить следующие проблемы в данном направлении:

- отсутствие формализованных механизмов обработки данных с целью повышения уровня и качества жизни граждан;
- недостаточный уровень доступности, качества и актуальности государственных

данных, необходимых для перехода на цифровое взаимодействие;

- отсутствие инфраструктуры, способной обеспечить унифицированный, безопасный, быстрый и удобный обмен данными между всеми участниками;

- отсутствие стандартов и решений в сфере информационной безопасности, в том числе криптографии, для обеспечения безопасного обмена данными между государственными органами и коммерческими компаниями;

- отсутствие соответствующей нормативной правовой базы [2].

Эти факторы негативно сказываются как для граждан, предпринимателей, так и на органы государственной власти. К числу проблем можно отнести также и достаточно высокий уровень расходов, которые связаны с обработкой бумажных документов, а также необходимостью личного присутствия граждан, ручной проверки и подтверждения предоставления данных, и низкая эффективность внутренних бизнес-процессов организаций, которые связаны с аналитикой данных (скоринг, риск-менеджмент, оценка просроченной задолженности, подготовка отчетности и т.д.), низкое качество клиентского опыта, снижение конверсии, недоступность части услуг для отдельных групп клиентов (например, услуг, требующих личного присутствия (подача документов, идентификация), для граждан, проживающих в труднодоступных районах), сложность персонализации продуктов и услуг на основе данных о физическом лице, полученных или актуализированных из внешних источников, и отсутствие у гражданина возможности управления выданными соглашениями в электронном виде и др.

Представляется целесообразным рассмотреть возможность внесения следующих изменений в законодательство Российской Федерации в части развития концепции «цифрового профиля»:

1. Сегодня законодатель предусматрива-

ет создание реестра согласий на обработку персональных данных гражданина, но в рамках них, к сожалению, не происходит реализация технологической возможности для гражданина отслеживать, какие органы государственной власти или организации используют персональные данные гражданина. Не устанавливается взаимодействие Цифрового профиля с первоначальными реестрами данных, в той части, когда запрос на использование данных направляется в первоначальный источник. Таким образом, гражданин не может полностью отследить через систему Цифрового профиля движения своих данных, что может обуславливать определенными злоупотреблениями;

2. К сожалению, на сегодняшний день не выработаны основные принципы внесения изменений в реестры. Сегодня необходимо более четко прописать алгоритм таких изменений и организационно продумать весь процесс;

3. В процессе развития системы Цифрового профиля необходимо проработать и решить вопрос о технологических и функциональных аспектах их реализации. Не в полной мере выработаны технологические и функциональные особенности реализации права на забвение;

4. К сожалению, не решен вопрос и необходимо вносить соответствующие изменения в законодательство об обеспечении должной защиты прав граждан на персональные данные, которые были получены из цифрового профиля коммерческими организациями и обрабатываются ими в коммерческих и иных экономических целях. Явно защита персональных данных в этом случае должна носить особый характер, особенно в части защиты биометрических персональных данных [3-4]. Причем, важно не только предусматривать требования к информационным системам таких персональных данных и требованиям к их функционированию в коммерческих организациях, но и проработать на уровне ФЗ «О персональных данных» [5] и иные меры. Одной меры здесь явно недостаточно, поскольку крупные операторы таких персональных данных легко могут позволить выполнить жесткие требования к информационным системам персональных данных, а предприятия малого и среднего бизнеса не смогут обеспечить такую возможность. С другой стороны, если предусматривать большие штрафные санкции, которые логично могут

быть предусмотрены для защиты прав на персональные данные из цифрового профиля, то крупные игроки на рынке легко могут закладывать такие штрафы в риски, связанные с утечкой персональных данных;

5. Важно также предусмотреть в рамках системы Цифрового профиля возможность реализовать на его базе возможности взаимодействия граждан и коммерческих организаций без рассылки рекламных и иных сообщений, если у организации отсутствует согласия на обработку персональных данных;

6. Необходимо решить вопрос, связанный с признанием юридической значимости данных Цифрового профиля, возможность их официального признания и использования в качестве официальных данных в тех или иных случаях, в том числе в качестве доказательств;

7. В связи с тем, что в рамках цифрового профиля гражданин может предоставить право использовать свои персональные данные той или иной организации для получения через нее государственной услуги, важно установить требования к коммерческим и некоммерческим организациям, в которые может обратиться заявитель за организацией предоставления государственных услуг. В рамках предлагаемых требований необходимо установить, как критерии для коммерческих и некоммерческих организаций, так и критерии для государственных услуг, которые могут предоставляться через инфраструктуру коммерческих и некоммерческих организаций гражданам. В качестве них могут быть предложены: количество принятых от заявителей запросов о предоставлении государственной услуги превышает в год (не менее 100-150 тысяч); организация предоставления государственной услуги в организации способствует повышению доли граждан, имеющих доступ к получению такой услуги; для получения услуг и сервисов организации используется результат предоставления государственной услуги либо сфера деятельности организации связана с получением государственной услуги и др.

Полагаем, что данные и другие предложения по развитию системы Цифрового профиля необходимо реализовать на уровне специально разработанных постановлений Правительства Российской Федерации, в которых бы были утверждены требования к организациям, которые получают для своих целей данные о гражданах из Цифрового про-

филя, а также основные требования к коммерческим и некоммерческим организациям, в которые может обратиться заявитель за организацией предоставления государственных услуг, условия предоставления таких услуг и критерии отбора указанных организаций. Ответственными федеральными органами исполнительной власти при этом должны быть Минцифры России, Минэкономразвития России.

При предоставлении персональных данных из цифрового профиля коммерческим и некоммерческим организациям важно закрепить ряд базовых положений:

– организации, предоставляющие государственные услуги и получающие персональные данные о гражданах обязаны обеспечивать защиту информации, доступ к которой ограничен в соответствии с требованиями законодательства Российской Федерации в области персональных данных, а также соблюдать режим обработки и использования персональных данных, в том числе и их работники;

– организации вправе использовать результаты предоставления государственных услуг и информации, ставшей доступной в результате предоставления государственных услуг заявителю, в том числе передавать их

третьим лицам, только при наличии информированного согласия заявителя на такое использование, за исключением случаев, когда такие результаты или информация в соответствии с федеральными законами являются общедоступной информацией;

– согласие заявителя оформляется в письменной форме посредством подписания документа на бумажном носителе или с использованием электронных документов, подписанных электронной подписью в соответствии с требованиями Федерального закона «Об электронной подписи», в том числе посредством проставления отметки (галочки) в таком согласии при условии ее проставления заявителем, аутентифицированным в информационной системе организации;

– организация не вправе обуславливать возможность получения государственной услуги заявителем обязанностью предоставить согласие на использование результатов предоставления государственных услуг и информации, ставшей доступной в результате предоставления государственных услуг.

Эти и другие меры будут способствовать развитию системы цифрового профилирования в Российской Федерации, а также обеспечению и защите прав граждан на защиту персональных данных.

Литература

1. Полякова Т. А. Проблемы правового обеспечения информационной безопасности в процессе использования цифровых технологий в глобальной цифровой среде / Т. А. Полякова, А. В. Минбалеев, И. С. Бойченко // Вестник Академии права и управления. – 2018. – № 3(52). – С. 32-36.
2. Полякова Т. А. Концептуальные подходы к правовому регулированию информационной безопасности в условиях цифровизации и трансформации права / Т. А. Полякова, А. В. Минбалеев, И. С. Бойченко // Вестник УрФО. Безопасность в информационной сфере. – 2019. – № 3(33). – С. 64-68.
3. Методические рекомендации Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации «Сценарии использования инфраструктуры Цифрового профиля. Версия 1.2» от 2 апреля 2021 г. URL: <https://digital.gov.ru/uploaded/presentations/stsenariiispolzovaniyatspv12.pdf> (дата обращения: 20.04.2021 г.).
4. Брызгин, А. А. Правовой режим биометрических персональных данных / А. А. Брызгин, А. В. Минбалеев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 2(4). – С. 35-41.
5. Захаров, М. Н. Правовая защита персональных данных / М. Н. Захаров, А. В. Минбалеев // Безопасность информационного пространства: сборник трудов XIII Всероссийской научно-практической конференции студентов, аспирантов и молодых учёных, Челябинск, 26–28 ноября 2014 года / Министерство образования и науки Российской Федерации, Южно-Уральский государственный университет, Кафедра «Безопасность информационных систем». – Челябинск: Издательский центр ЮУрГУ, 2015. – С. 211-215.
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

References

1. Polyakova T. A. Problemy pravovogo obespecheniya informacionnoj bezopasnosti v processe ispol'zovaniya cifrovyyh tekhnologij v global'noj cifrovoj srede / T. A. Polyakova, A. V. Minbaleev, I. S. Bojchenko // Vestnik Akademii prava i upravleniya. – 2018. – № 3(52). – S. 32-36.

2. Polyakova T. A. Konceptual'nye podhody k pravovomu regulirovaniyu informacionnoj bezopasnosti v usloviyah cifrovizacii i transformacii prava / T. A. Polyakova, A. V. Minbaleev, I. S. Bojchenko // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2019. – № 3(33). – S. 64-68.

3. Metodicheskie rekomendacii Ministerstva cifrovogo razvitiya, svyazi i massovyh kommunikacij Rossijskoj Federacii «Scenarii ispol'zovaniya infrastruktury Cifrovogo profilya. Versiya 1.2» ot 2 aprelya 2021 g. URL: <https://digital.gov.ru/uploaded/presentations/stsenariispolzovaniyatspv12.pdf> (data obrashcheniya: 20.04.2021 g.).

4. Bryzgin, A. A. Pravovoj rezhim biometricheskikh personal'nyh dannyh / A. A. Bryzgin, A. V. Minbaleev // Vestnik UrFO. Bezopasnost' v informacionnoj sfere. – 2012. – № 2(4). – S. 35-41.

5. Zaharov, M. N. Pravovaya zashchita personal'nyh dannyh / M. N. Zaharov, A. V. Minbaleev // Bezopasnost' informacionnogo prostranstva: sbornik trudov XIII Vserossijskoj nauchno-prakticheskoj konferencii studentov, aspirantov i molodyh uchyonyh, Chelyabinsk, 26–28 noyabrya 2014 goda / Ministerstvo obrazovaniya i nauki Rossijskoj Federacii, YUzhno-Ural'skij gosudarstvennyj universitet, Kafedra «Bezopasnost' informacionnyh sistem». – Chelyabinsk: Izdatel'skij centr YUUrGU, 2015. – S. 211-215.

6. Federal'nyj zakon ot 27.07.2006 № 152-FZ «O personal'nyh dannyh» // Sobranie zakonodatel'stva RF. 2006. № 31 (1 ch.). St. 3451.

МИНБАЛЕЕВ Алексей Владимирович, доктор юридических наук, профессор, зав. кафедрой информационного права и цифровых технологий, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). 123001, г. Москва ул. Садовая-Кудринская, 9.; профессор кафедры теории государства и права, конституционного и административного права, Южно-Уральский государственный университет. 454080, г. Челябинск, пр. Ленина, 76. E-mail: alexmin@bk.ru.

MINBALEEV Aleksey Vladimirovich, Doctor of Sciences (Law), Professor, head Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL). Sadovaya-Kudrinskaya st., 9, Moscow, 123001.; Professor of the Department of Theory of State and Law, Constitutional and Administrative Law, South Ural State University. 76 Lenin Ave., Chelyabinsk, 454080. E-mail: alexmin@bk.ru.