

УДК 343.97

ПРОБЛЕМЫ ПЕРСОНИФИКАЦИИ ДАННЫХ В ЦИФРОВУЮ ЭПОХУ

Гиреев Джафар Темирланович,¹
аспирант,

e-mail: Gireev166@mail.ru,

¹Российская академия народного хозяйства и государственной службы
при Президенте РФ, Москва, Россия

В статье анализируются научные подходы и нормы российского законодательства о персональных данных. При этом персональные данные рассматриваются как правовая категория, включающая в себя массив информации, позволяющей отличать одного человека от другого, показывающей способности, которыми обладает субъект персональных данных, а также указывающей на его конституционно-правовой и административно-правовой статус.

Ключевые слова: государство, цифровизация, персональные данные, цифровые права, информационное общество, цифровые технологии

PROBLEMS OF DATA PERSONIFICATION IN THE DIGITAL AGE

Gireev J.T.,¹

postgraduate,

e-mail: Gireev166@mail.ru,

¹Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia

The article analyzes the scientific approaches and norms of the Russian legislation on personal data. At the same time personal data is considered as a legal category, which includes an array of information allowing to distinguish one person from another; showing the abilities, that the subject of personal data has, and also indicating its constitutional and administrative status.

Keywords: state, digitalization, personal data, digital rights, information society, digital technologies

DOI 10.21777/2587-9472-2020-3-25-28

В социальной жизни каждый человек в той или иной мере участвует в качестве отдельного субъекта в различных общественных отношениях, связанных с сохранением в секрете своих персональных данных. Согласно некоторым авторам, наиболее часто такие отношения возникают в сферах финансов, образования, здравоохранения, при осуществлении адвокатской и нотариальной деятельности, расследовании уголовных дел. Зачастую в процессе развития данных отношений возникают конфликтные ситуации, которые, по мнению Э.В. Талапиной, могут быть классифицированы на несколько групп по основанию того, с чем вступает в противоречие защита персональных данных при ее осуществлении [1, с. 128].

1. Защита персональных данных и публичный интерес.

В большинстве государств мира установлены специальные правила хранения персональных данных своего населения. В связи с этим зачастую возникает вопрос о том, кто является их собственником, поскольку интересы субъекта данных противопоставляются интересам национальной безопасности и другим публично-правовым интересам государства. Так, Федеральным законом РФ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»¹ установлена обязанность

¹ См.: Федеральный закон РФ от 21.07.2014 г. № 242-ФЗ (ред. от 31.12.2014 г.) «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // Российская газета. – 2014. – № 163.

операторов обеспечивать запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории страны, при сборе персональных данных, в том числе посредством сети Интернет. При этом следует сказать, что не только Россия, но и множество других государств, например Япония, Турция, Аргентина, обязывают операторов электронных ресурсов осуществлять локализацию персональных данных своих пользователей [2, с. 142].

Названный закон не предусматривает обязанность получения согласия субъекта данных на их передачу за пределы России, что не соответствует положениям ст. 23 и ч. 4 ст. 29 Конституции РФ. Неисполнение операторами персональных данных этой обязанности влечет за собой возможность привлечения их к административной ответственности согласно ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных» Кодекса РФ об административных правонарушениях (далее – КоАП РФ). Вместе с тем с иностранной компании-оператора, не открывшей своего представительства в России, взыскать административный штраф, предусмотренный санкцией данной статьи КоАП РФ, практически невозможно [3].

2. Защита персональных данных и информация ограниченного доступа.

Персональные данные и информация ограниченного доступа являются взаимосвязанными между собой правовыми категориями, хотя и относятся соответственно к частному и публичному праву. Из данного обстоятельства вытекает конфликтная ситуация, разрешать которую пришлось Конституционному суду РФ (далее – КС РФ).

Гражданин Круглов обратился в государственное бюджетное учреждение здравоохранения с просьбой удалить со своей базы данных его персональные данные, обрабатываемые, по его мнению, противозаконно. Однако в этом ему было отказано со ссылкой на то, что законодательством такая обязанность для медицинских учреждений не предусмотрена. Гражданин Круглов обратился в КС РФ за разъяснением соответствующих положений законодательства Российской Федерации о персональных данных. На это КС РФ указал, что учреждения здравоохранения вправе хранить информацию о состоянии здоровья своих пациентов только с целью обеспечения их права на его охрану и качественное оказание неотложной медицинской помощи. При этом информация такого характера должна обеспечиваться соблюдением врачебной тайны. В этой связи требование пациента как субъекта персональных данных об удалении информации о состоянии своего здоровья с электронной базы данных медицинского учреждения не подлежит удовлетворению².

Конституционный суд РФ оценивает персональные данные как важнейшую информацию конфиденциального характера, равную по своей значимости банковской, нотариальной, адвокатской тайне, тайне исповеди и другим тайнам человека, охраняемым законом. Кроме того, КС РФ указывает, что запрет на их разглашение обусловлен интересами нераспространения сведений, составляющих соответствующую тайну.

В своем Определении от 06.10.2015 г. № 2443-О КС РФ указал, что разглашение персональных данных, как и иных сведений, в любой мере относящихся к охраняемой законом тайне, является посягательством на права личности, представляющим общественную опасность»³.

3. Защита персональных данных и технологии обработки больших данных.

По общему правилу, субъект персональных данных должен давать письменное согласие на их обработку. Данное положение представляется обоснованным. Вместе с тем последствия такого согласия в силу специфики технологий больших данных, применяемых в настоящее время, зачастую предугадать невозможно, что делает согласие субъекта персональных данных не более чем фикцией, поэтому его нельзя оценивать как главное основание, придающее правомерность их обработке.

² См.: Определение Конституционного суда РФ от 16.07.2013 г. № 1176-О «Об отказе в принятии к рассмотрению жалобы гражданина Круглова Александра Геннадьевича на нарушение его конституционных прав пунктом 4 части 2 статьи 10 Федерального закона "О персональных данных"» [Электронный ресурс]. – Режим доступа: <http://www.legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-16072013-n-1176-o-ob> (дата обращения: 21.04.2021).

³ См.: Определение Конституционного суда РФ от 06.10.2015 г. № 2443-О «По жалобе граждан Динзе Дмитрия Владимировича и Сенцова Олега Геннадьевича на нарушение их конституционных прав положениями пункта 3 части второй статьи 38, части третьей статьи 53 и статьи 161 Уголовно-процессуального кодекса Российской Федерации» [Электронный ресурс]. – Режим доступа: <http://www.garant.ru/products/ipo/prime/doc/71145924> (дата обращения: 21.04.2021).

Одним из способов предотвращения потенциальных нарушений является процедура обезличивания персональных данных⁴. Однако российское законодательство содержит лишь предложения общего характера, обращенные к контролерам и обработчикам персональных данных, руководствоваться последними достижениями науки и техники по применению методов обезличивания таких данных.

4. Защита персональных данных, свобода и нейтральность интернета.

Нейтральность интернета является одним из его основополагающих принципов. Согласно этому принципу, оператор данной электронной сети не должен устанавливать никаких приоритетов и привилегий при предоставлении доступа к веб-сайтам. Скорость доступа к ним должна быть равной для всех пользователей вне зависимости от содержания сайтов, владельцами которых они являются. Наиболее остро данное противоречие проявляется при обнародовании лживых (фейковых), а также устаревших новостей, что не может не касаться и персональных данных.

5. Защита персональных данных и другие права человека.

Наиболее распространенными конфликтами являются конфликты между правом на защиту персональных данных и правом на свободу выражения своей точки зрения по тому или иному вопросу. При установлении равновесия между данными правами должно учитываться следующее:

- 1) имеет или нет противоречие общественный интерес;
- 2) является ли лицо, оказавшееся в центре конфликта, публичным и насколько;
- 3) является ли распространяемая информация достоверной и как она была получена;
- 4) каковы последствия обнародования информации;
- 5) насколько суровым является поименное наказание.

Данный конфликт трудно разрешим, поскольку универсального пути его разрешения нет. Данное обстоятельство сказалось на содержании Общего регламента по защите персональных данных⁵ (далее – Регламент). Так, в ст. 85 «Обработка и свобода выражения мнений и информации» Регламента закреплена обязанность государств, являющихся членами Европейского союза, в законодательном порядке согласовать право на защиту персональных данных и право на свободу выражения мнений и распространения информации [4, с. 246].

6. Защита персональных данных и права работодателя.

В последние годы возникла такая категория споров между работодателями и работниками, как споры, связанные с мониторингом электронной почты последних. Суть данного вопроса КС РФ раскрыл в своем Постановлении от 26.10.2017 г. № 25-П «По делу о проверке конституционности п. 5 ст. 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова»⁶.

Работодатель истолковал отправление Сушковым корпоративной информации с электронного адреса предприятия на свой личный электронный адрес как разглашение конфиденциальной информации. Суд при рассмотрении данного дела принял сторону работодателя. Свою точку зрения суд обосновал действием пользовательского соглашения, согласно которому работодатель вправе как закрывать, так и разрешать доступ к информации, сосредоточенной на его почтовом адресе. Тем самым КС РФ предоставил право организациям включать в свои локальные нормативные правовые акты запрет на передачу ее работниками какой-либо информации с корпоративного электронного адреса на свой личный электронный адрес.

Таким образом, использование гражданами цифровых технологий существенно сокращает время получения ими искомой информации, которая хранится в информационных массивах (учетах) элек-

⁴ См.: Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ от 05.09.2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» // Российская газета. – 2013. – № 208.

⁵ См.: Регламент № 2016/679 Европейского парламента и Совета Европейского союза «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент о защите персональных данных)» [рус., англ.] (принят в г. Брюсселе 27.04.2016 г.) [Электронный ресурс]. – Режим доступа: <http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=60453#09554366703568662> (дата обращения: 16.05.2021).

⁶ См.: Постановление Конституционного суда РФ от 26.10.2017 г. № 25-П «По делу о проверке конституционности пункта 5 статьи 2 Федерального закона "Об информации, информационных технологиях и о защите информации" в связи с жалобой гражданина А.И. Сушкова» // Вестник Конституционного суда РФ. – 2017. – № 6.

тронных систем. Вводится туда информация их операторами, которые ее же и обрабатывают. По причине того, что применение цифровых технологий существенно облегчает жизнь человеку, она не может быть закрытой. В цифровую эпоху личная информация, к которой относятся и персональные данные конкретного человека, является товаром, соответственно, она подлежит защите от попыток третьих лиц неправомерно завладеть ею с целью использования в своих корыстных целях. Высокий уровень развития в настоящее время цифровых технологий сделал идентификацию (отождествление) личности человека безошибочной в силу того, что он обладает множеством присущих только ему (субъекту данных) признаков. При этом его идентификация с использованием цифровых технологий все более и более ускоряется, а также упрощается.

Список литературы

1. *Талапина Э.В.* Защита персональных данных в цифровую эпоху: российское право в европейском контексте // Труды Института государства и права РАН. – 2018. – Т. 13. – № 5. – С. 117–150.
2. *Иванов А.А.* Хранение персональных данных за рубежом с точки зрения российского права // Закон. – 2015. – № 1. – С. 134–143.
3. *Жердина С.А.* Локализация персональных данных россиян для иностранных компаний // ЭЖ-Юрист. – 2017. – № 3.
4. *Постникова Е.В.* Некоторые аспекты правового регулирования защиты персональных данных в рамках внутреннего рынка Европейского союза // Право. Журнал Высшей школы экономики. – 2018. – № 1. – С. 234–254.

References

1. *Talapina E.V.* Zashchita personal'nyh dannyh v cifrovuyu epohu: rossijskoe pravo v evropejskom kontekste // Trudy Instituta gosudarstva i prava RAN. – 2018. – T. 13. – № 5. – S. 117–150.
2. *Ivanov A.A.* Hranenie personal'nyh dannyh za rubezhom s tochki zreniya rossijskogo prava // Zakon. – 2015. – № 1. – S. 134–143.
3. *Zherdina S.A.* Lokalizaciya personal'nyh dannyh rossiyan dlya inostrannyh kompanij // EZh-Yurist. – 2017. – № 3.
4. *Postnikova E.V.* Nekotorye aspekty pravovogo regulirovaniya zashchity personal'nyh dannyh v ramkah vnutrennego rynka Evropejskogo soyuza // Pravo. Zhurnal Vysshej shkoly ekonomiki. – 2018. – № 1. – S. 234–254.