DOI 10.25799/NI.2023.10.22.010
УДК 342.723:004

Правовые механизмы защиты персональных данных в информационно-телекоммуникационных системах

Е.А. Свиридова,
кандидат юридических наук
доцент Департамента правового регулирования
экономической деятельности юридического факультета
Финансового университета при Правительстве РФ
Россия, Москва
esviridova@fa.ru

В статье рассматриваются возможные пути совершенствования механизмов защиты персональных данных в информационно-телекоммуникационных системах, в том числе при их трансграничной передаче. Целью исследования является анализ теоретических и практических аспектов защиты персональных данных в информационно-телекоммуникационных системах. Делается вывод о крайне широком законодательном понятии персональных данных, что приводит к неопределенности правоприменения. На основе тезиса о необходимости учета всех сведений о субъекте персональных данных в совокупности, включая данные стороннего оператора, сформулировано предложение о необходимости уточнения критериев данных, относящихся косвенно к определенному или определяемому физическому лицу. Исследуется вопрос о необходимости разработки мер по совершенствованию механизма защиты платежных данных.

Ключевые слова: *персональные данные, право на неприкосновенность частной жизни, трансграничная передача данных, оператор персональных данных, субъект персональных данных.*

Введение. Защита персональных данных стоит на стыке интересов публичных и частных, когда, с одной стороны, государство заинтересовано в обеспечении безопасности, а с другой, — возникает необходимость соблюдения прав и свобод личности. Кроме того, персональные данные, изначально принадлежащие частному субъекту, в процессе их обработки и хранения перестают быть монополией их носителя. Право субъекта персональных данных на распоряжение собственными персональными данными ограничивается публично-правовыми интересами локализации персональных данных, в том числе интересами национальной безопасности [5].

В области информационно-телекоммуникационных систем не до конца проработанным остается механизм защиты персональных данных, в том числе при их трансграничной передаче. Особую актуальность эта проблема приобрела в последнее время, когда участились случаи хакерских атак с кражей данных военнослужащих и последующим размещением информации о месте их жительства и сведений об их семьях в открытом доступе. Сервисы, на которых незаконно распространяются такие данные, как правило, зарегистрированы на территории иностранных юрисдикций, в связи с чем отсутствует возможности осуществления защиты персональных данных в соответствии с нормами российского законодательства. В условиях текущей внешнеполитической ситуации и новых санкций со стороны недружественных стран требуется разработать действенный механизм защиты персональных данных, в том числе при их трансграничной передаче.

Понятие персональных данных в доктрине и судебной практике. Понятие персональных данных, представленное в законе, сформулировано чрезвычайно широко, что часто порождает неясность правоприменения. Действующая законодательная формулировка позволяет выделить две основные категории персональных данных: общие (содержащие любые сведения, касающиеся прямо или косвенно определенного или определяемого субъекта персональных данных) и специальные (включающие сведения, определяющие расовую и национальную принадлежность, политические взгляды, религиозные или философские убеждения, состояние здоровья, иные данные о личной жизни физического лица).

Действующая дефиниция персональных данных чрезвычайно широко определяет потенциально возможные данные, которые можно было бы отнести к категории персональных. По мнению А.И. Савельева, существует прямая зависимость между определением того, что можно отнести к персональным данным, и конкретными обстоятельствами и вероятными взаимосвязями отдельных фрагментов информации [4]. А.В. Мунтян считает, что при отнесении тех или иных данных к персональным большое значение имеет контекст [2].

С учетом той личной информации, которую пользователи загружают в социальные сети, необходимо определить, вся ли она подпадает под понятие персональных данных, обработка и использование которых требует получения согласия пользователя. Поскольку закон о персональных данных относит к последним в том числе сведения, которые косвенно могут ассо-

циироваться с субъектом персональных данных, судебная практика и Роскомнадзор справедливо указывают в числе персональных данных следующую информацию: данные геолокации; аудио-, визуальную информацию; данные, позволяющие определить профессиональные интересы субъекта; данные с камер видеонаблюдения; данные пользовательской аналитики, собираемые сервисами «Яндекс.Метрика» и «Google Аналитика»; cookie файлы; история заказов в интернет-магазинах; IP-адрес.

В деле Patrick Breyer против Федеративной республики Германия Европейский суд справедливости разъяснил понятие косвенной связи данных с субъектом персональных данных: такие данные не всегда достаточны сами по себе для персонификации лица [6].

Таким образом, косвенная ассоциативная связь данных с их субъектом означает отсутствие четкого и однозначного вывода о связанности с конкретным субъектом персональных данных, но позволяет идентифицировать субъекта на основе анализа совокупности таких данных. Поэтому любые сведения о действиях лица в сети Интернет, в частности история поисковых запросов, история браузера, история перехода по ссылкам контекстной рекламы, данные о трафике (метаданные) следует отнести к категории персональных данных.

На практике разные операторы обладают различным массивом данных. В связи с этим для определения статуса таких данных обычно используются данные конкретного оператора. Однако, когда данные относятся к субъекту лишь косвенно, крайне важно для понимания возможности идентификации субъекта за счет таких данных рассматривать все сведения в совокупности, включая и те данные, которыми владеет сторонний оператор. Учитывая развитие технологии больших данных, позволяющей взаимодействовать операторам данных в целях их совместной обработки, целесообразно в ст. 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» уточнить критерии данных, относящихся косвенно к определенному или определяемому физическому лицу. Такими критериями предлагается признать возможность с их помощью идентифицировать конкретного субъекта при взаимодействии с данными, принадлежащими стороннему оператору, и наличие у оператора данных потенциального доступа к данным стороннего оператора. Данное дополнение закона позволит конкретизировать понятие персональных данных и обеспечить их защиту в информационно-телекоммуникационной среде.

Федеральным законом от 14.07.2022 № 266-ФЗ были внесены изменения в Федеральный закон «О персональных данных» [3]. В частности, с 1 марта 2023 г. у операторов персональных данных появится обязанность предварительно сообщать уполномоченному органу по защите прав субъектов персональных данных о планируемой трансграничной передаче данных. До этого момента оператор персональных данных должен получить от уполномоченных органов, физических и юридических лиц иностранного государства, на территорию которого планируется осуществить трансграничную передачу данных, информацию о принимаемых ими мерах по защите передаваемых персональных данных и особенностях правового регулирования персональных данных в таком государстве.

В случае выявления угрозы обороне страны, безопасности государства, нарушения основ конституционного строя уполномоченный орган по защите прав субъектов персональных данных наделяется правом на запрет или ограничение трансграничной передачи данных. При отрицательном решении уполномоченного органа по защите прав субъектов персональных данных на оператора налагается обязанность незамедлительно уничтожить ранее переданные ему персональные данные. Таким образом, рассмотренные поправки в закон о персональных данных устанавливают механизм защиты персональных данных, распространяемых в информационно-телекоммуникационных сетях путем размещения их на серверах, расположенных за пределами территории Российской Федерации.

Механизмы защиты платежных данных. В связи с появлением новых цифровых платежных способов, а также ограничениями, наложенными на нашу страну в рамках санкций, неизбежны глубокие преобразования в системе расчетов. Об этом свидетельствует недавно принятая в России Концепция законодательного регламентирования механизмов организации оборота цифровых валют, которая определяет цели и задачи государственного регулирования деятельности по организации оборота цифровых валют [1]. Концепция предусматривает использовать в целях мониторинга криптовалютных транзакций цифровой сервис «Прозрачный блокчейн» Росфинмониторинга. Указанный сервис может проводить идентификацию участника расчетов с использованием данных из открытых источников сети Интернет, социальных сетей и Даркнет, а также составлять профили участников и давать оценку их роли в экономической деятельности на основе мониторинга собранной информации. Идентификация участников операции обмена цифровой валюты включает, в том числе, персональные данные физического лица (имя, адрес, дата рождения, адрес электронной поч-

ты, номер телефона, номер телефона устройства, имя пользователя, пароль, данные банковского счета, копии документов, удостоверяющих личность, фотографии клиента, информацию о транзакции, включая дату, время, сумму, используемые валюты, данные получателя и отправителя). Оператор обмена цифровых валют наделяется обязанностью по предоставлению данных о планируемой к совершению операции организатору системы обмена цифровых валют. Концепция предусматривает внесение изменений в отдельные законодательные акты Российской Федерации в связи с ее реализацией, однако в их перечне отсутствует Федеральный закон «О персональных данных».

В этом контексте, когда платежные данные выходят за рамки традиционных безопасных денежных потоков, а обращаются в сети Интернет для многих (не всегда идентифицируемых) цифровых целей, необходимо разработать пакет мер по совершенствованию механизма защиты платежных данных.

Для начала необходимо определить платежные данные как совокупность персональных данных, используемых при предоставлении платежной услуги физическому лицу, включая дополнительные данные, такие как геолокация, контекстные данные (в частности, детали совершенных транзакций).

Платежные данные можно разделить на три основные категории:

1) фактические платежные данные — сумма транзакции, дата и время платежа, данные плательщика, данные получателя средств;

2) данные о транзакциях — характеристика приобретенных товаров, работ, услуг, дата и место покупки;

3) контекстные данные — данные о «покупательском поведении» клиента, включая геолокацию, характеристики терминала, используемого для онлайн-покупки, характеристики товаров, которые были просмотрены до начала покупки, время, затраченное на поиск товара.

В целях повышения безопасности и обеспечения защиты данных при осуществлении расчетов с использованием новых цифровых платежных систем следует разработать специальный правовой подход, применяемый к обработке, распространению, предоставлению, использованию и повторному использованию платежных данных. Необходимо учитывать широкий спектр данных, обрабатываемых при проведении расчетов с помощью платежных систем, а также повторное использование платежных данных, и ограничить использование платежных данных оператором и организатором обмена цифровых валют теми данными, которые необходимы в целях выявления вероятности участия участников криптовалютного рынка в противоправной деятельности, в том числе в целях определения фактов легализации и сокрытия средств, полученных преступным путем. Но в связи с реализацией указанных выше целей обработка контекстных платежных данных оператором и организатором обмена цифровых валют не является необходимой для осуществления платежных операций и противоречит принципу неприкосновенности частной жизни.

В связи с широким распространением киберпреступлений, в том числе связанных как с мошенничеством в сфере электронных платежей, так и с кражей персональных данных, необходимо интегрировать задачи информационной безопасности во все проекты, связанные с информационно-телекоммуникационной инфраструктурой. В настоящее время токенизация данных в целях реализации платежа видится наиболее эффективным решением проблем безопасности. Токенизация — это метод, позволяющий заменить персональные платежные данные, такие как номер счета или номер банковской карты, случайно генерируемыми одноразовыми данными (токенами), использование которых ограничено однократным применением и может быть лимитировано по времени. Помимо этого, ограниченный срок хранения данных ограничивает и последующее их использование.

Таким образом, практика токенизации может обеспечить лучшую защиту платежных данных. В случае взлома какого-либо участника платежной цепочки, который необходимо учитывать при анализе рисков, использованный номер становится непригодным для употребления. Данное решение обеспечивает финансовую безопасность плательщика, одновременно защищая его с точки зрения конфиденциальности данных. Оно также обеспечивает защиту оператора платежной системы, минимизируя риски мошеннических действий и повторного использования номера без ведома владельца. Однако для внесения ясности в практику применения необходимо разработать практические рекомендации для органов, осуществляющих регулирование, контроль и надзор за деятельностью провайдеров услуг виртуальных активов по токенизации платежных данных, включая используемые методы и передовую практику.

Выводы. В рамках поправок к Конституции РФ от 14 марта 2020 г. к предмету ведения Российской Федерации было отнесено обеспечение безопасности личности, общества и государства при применении информационных технологий и обороте цифровых данных. Паспорт федерального проекта «Нормативное

регулирование цифровой среды» требует создания благоприятных правовых условий для сбора, хранения и обработки данных с использованием новых технологий. Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы указывает на необходимость обеспечения баланса между своевременным внедрением современных технологий обработки данных и защитой прав граждан, включая право на личную и семейную тайну. Несмотря на то, что последние поправки в Федеральный закон «О персональных данных» максимально гармонизировали понятие персональных данных в соответствии с СДСЕ № 108 и GDRP, на практике до сих пор возникают трудности при интерпретации понятия «персональные данные».

В связи с тем, что косвенная ассоциативная связь данных с их субъектом не позволяет сделать однозначный вывод о связанности с конкретным субъектом персональных данных, но дает возможность идентифицировать субъекта на основе анализа совокупности таких данных, предлагается для понимания возможности идентификации субъекта за счет таких данных рассматривать все сведения в совокупности, включая и те данные, которыми владеет сторонний оператор.

Платежные данные представляется возможным разделить на три категории: фактические платежные данные, данные о транзакциях, контекстные данные. Следует ограничить использование платежных данных оператором и организатором обмена цифровых валют теми данными, которые необходимы в целях выявления вероятности участия участников криптовалютного рынка в противоправной деятельности, в том числе в целях определения фактов легализации и сокрытия средств, полученных преступным путем.

Список литературы

1. Концепция законодательного регламентирования механизмов организации оборота цифровых валют // Правительство Российской Федерации [сайт] — URL: http://static.government.ru/media/files/Dik7wBqAubc34ed649ql2Kg6HuTANrqZ.pdf (дата обращения: 08.11.2022).

2. Мы вступили в эпоху цифрового огораживания и национализации (персональных) данных [Интервью с А.В. Мунтяном] // Закон. 2022. № 3. С. 8—15.

3. 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» : Федеральный закон от 14.07.2022 № 266-ФЗ // Собрание законодательства РФ. 2022. № 29 (ч. III). Ст. 5233.

4. *Савельев, А.И*. Электронная коммерция в России и за рубежом: правовое регулирование. - 2-е изд. / А.И. Савельев. М. : Статут, 2016. 640 с.

5. *Талапина, Э.В.* Защита персональных данных в цифровую эпоху. Российское право в европейском контексте / Э.В. Талапина // Труды Института государства и права РАН. 2018. Т. 13. № 5. С. 137.

6. Patrick Breyer v. Bundesrepublik Deutschland, ECJ, Case C-582/14, 19 October 2016 // ECLI:EU:C:2016:779.

References

1. The concept of legislative regulation of the mechanisms for organizing the circulation of digital currencies [website] — URL: http://static.government.ru/media/files/Dik7wBqAubc34ed649ql2Kg6HuTANrqZ.pdf(date of access: 08.11.2022).

2. We have entered the era of digital fencing and nationalization of (personal) data [Interview with A.V. Muntyan] // Law. 2022. No. 3. S. 8-15.

3. On Amending the Federal Law "On Personal Data", Certain Legislative Acts of the Russian Federation and Recognizing Part Fourteen of Article 30 of the Federal Law "On Banks and Banking Activity: Federal Law No. 266-FZ of July 14, 2022" as invalid // Legislation Collection RF. 2022. No. 29 (Part III). Article 5233.

4. Saveliev, A.I. Electronic commerce in Russia and abroad: legal regulation. - 2nd ed. / A.I. Saveliev. M. : Statut, 2016. 640 p.

5. Talapina, E.V. Protection of personal data in the digital age. Russian law in the European context / E.V. Talapina // Proceedings of the Institute of State and Law of the Russian Academy of Sciences. 2018. Vol. 13. No. 5. P. 137.

6. Patrick Breyer v. Bundesrepublik Deutschland, ECJ, Case C-582/14, 19 October 2016 // ECLI:EU:C:2016: 779.

Legal Mechanisms of Personal Data Protection in Information and Telecommunication Systems

Sviridova E.A.,
Cand. in Law, Assoc. Prof. of Dept.
of Legal Regulation of Economic Activity
at Financial University under the Government
of Russian Federation
Russia, Moscow
esviridova@fa.ru

The article discusses possible ways to improve the mechanisms of personal data protection in information and telecommunications systems, including their cross-border transfer. The purpose of the study is to analyze the theoretical and practical aspects of personal data protection in information and telecommunication systems. The conclusion is made about the extremely broad legislative concept of personal data, which leads to the uncertainty of law enforcement. Based on the thesis about the need to take into account all the information about the subject of personal data in aggregate, including the data of a third-party operator, a proposal is formulated on the need to clarify the criteria for data related indirectly to a specific or identifiable individual. The question of the need to develop measures to improve the mechanism of payment data protection is being investigated.

Keywords: *personal data, right to privacy, cross-border data transfer, personal data operator, personal data subject*