

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ КЛИЕНТОВ ПРИ ОКАЗАНИИ ФИНАНСОВЫХ УСЛУГ С ИСПОЛЬЗОВАНИЕМ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Балашов Владимир Андреевич

магистрант Финансового университета при Правительстве Российской Федерации, РФ, г. Москва

Федорова Ирина Анатольевна

научный руководитель, доцент Департамента международного и публичного права
Финансового университета при Правительстве Российской Федерации, РФ, г. Москва

LEGAL REGULATION OF THE PROTECTION OF PERSONAL DATA OF CLIENTS IN THE PROVISION OF FINANCIAL SERVICES USING FINANCIAL TECHNOLOGIES

Vladimir Balashov

*Undergraduate Financial University under the Government of the Russian Federation, Russia,
Moscow*

Irina Fedorova

*Scientific director, Associate Professor of the Department of International and Public Law of the
Financial University under the Government of the Russian Federation, Russia, Moscow*

Аннотация. В статье проводится анализ законодательной базы правового регулирования защиты персональных данных клиентов при оказании финансовых услуг с использованием финансовых технологий. Проводится анализ российской и зарубежной практики и опыта. Рассматриваются перспективы развития правового регулирования защиты персональных данных при использовании финтех услуг.

Abstract. The article analyzes the legal framework of the legal regulation of the protection of personal data of clients in the provision of financial services using financial technologies. The analysis of Russian and foreign practice and experience is carried out. The prospects for the development of legal regulation of personal data protection when using fintech services are considered and made conclusions.

Ключевые слова: финтех, персональные данные, киберпреступления, цифровизация, цифровая личность, цифровая экономика, киберстрахование.

Keywords: fintech, personal data, cybercrime, digitalization, digital identity, digital economy, cyber insurance.

Финансовые технологии, по-другому – «финтех услуги» или «финтех», это активно развивающаяся отрасль в сфере предоставления населению финансовых средств и услуг. Привлекательность финансовых технологий в первую очередь связана с удобством, высоким качеством, отсутствием посредников для совершения операций, а также анонимностью и прозрачностью самих платежей [1]. Согласно нормам Федерального закона «О совершении сделок с использованием финансовых платформ», все существующие финансовые платформы, которые напрямую относятся к финтех индустрии, должны обеспечивать защиту персональных данных пользователя такой платформы [2]. Ввиду того, что тема защиты персональных данных востребована во всех современных правоотношениях, в рамках новой финтех отрасли она становится как никогда актуальной. Так, несмотря на стремительное развитие финансовых технологий, правовое регулирование этих правоотношений значительно «опаздывает», так как на сегодняшний день в Российской Федерации нет четкого законодательного подхода к регулированию этих правоотношений. И в этом аспекте интересно рассмотреть то, как именно защищаются персональные данные клиентов в данной сфере деятельности.

Финтех (финансовые технологии) – это предоставление финансовых услуг и сервисов с использованием инновационных технологий, таких как «Big Data», искусственный интеллект, машинное обучение, роботизация, блокчейн, облачные технологии, биометрия и др [3]. Исходя из определения, инновации в сфере финансовых технологий условно можно разделить на несколько основных групп [1]:

1. Облачные системы. Представляют собой функциональные системы, которые оказывают финансовые услуги клиентам посредством сети «Интернет»;
2. Роботизация. Многие функциональные возможности финансовых инструментов и технологий переходят в режимы полной компьютеризации и информатизации, в том числе путем использования систем искусственного интеллекта, а также путем разработки специальных приложений для удобного и удаленного получения услуг клиентами;
3. Технология блокчейн. Эта технология сейчас используется практически повсеместно и представляет собой защищенную сеть (реестр) транзакций, которые хранятся в системе без централизации такого процесса (отдельные элементы системы обладают автономностью, что позволяет достичь большей степени безопасности данных).

Как уже говорилось, считается, что финансовые технологии рассматриваются с исключительно положительной точки зрения – услуги становятся доступными, а, следовательно, они могут привлечь большее количество потенциальных клиентов. Однако исходя из приведенной классификации современных финтех услуг, становится очевидно, что все они непосредственно связаны с цифровым пространством, а следовательно, повышается риск киберпреступлений, в том числе совершаемых в отношении персональных данных пользователей.

Отношения, которые возникают вследствие сбора, хранения и обработки персональных данных, регулируются различными нормативными правовыми актами. В Российской Федерации основным актом в данной сфере правоотношений является Федеральный закон «О персональных данных», в котором устанавливается необходимость защиты персональных данных граждан [4]. Данный акт непосредственно закрепляет нормы ответственности к субъектам, которые участвуют в процессе сбора, обработки и хранения персональных данных. При этом основная проблема этого акта заключается в непосредственных элементах юридической техники. Во-первых, отсутствие четкой терминологической основы (нет четких критериев того, какая информация будет относиться к категории «персональные данные»). В связи с этим судебная практика неоднозначна в вопросах определения информации, относящейся к персональным данным [5]. Во-вторых, отсутствие проработанного субъектного состава (в законодательстве Европейского союза выделяется широкий перечень субъектов правоотношений, тогда как российское законодательство устанавливает два субъекта – это «субъект персональных данных» и «оператор персональных данных»). В-третьих, отсутствие законодательно закрепленных особенностей защиты персональных данных в сфере финтех услуг.

Проблема нарушения безопасности данных является общемировой, а не только российской. Поэтому сегодня большинство исследователей склоняются к образованию нового сегмента – киберстрахования в России. Для примера, в США данная сфера функционирует уже более 10 лет (например компании Allianz). Основная проблема заключается в разработке достаточной системы защиты персональных данных, которые предоставляют клиенты для получения финтех-услуг. Например, в Индии, которая начала разработку единой государственной платформы «цифровой личности» значительно раньше, чем в России, уже столкнулась с рядом проблем, в том числе со слабой защитой персональных данных, когда третьими лицами был получен доступ к биометрической базе данных, которая использовалась клиентами для получения дотаций от правительства, идентификации клиентов в банке и др. [6]. Но есть и положительные примеры разработки отдельных финансовых технологий с высокой степенью защиты, например Apple Card, которая запущена в США [7].

Использование биометрических данных для идентификации пользователей в банковских приложениях распространено также и в Российской Федерации. При этом, на сегодняшний день речь идет уже больше о внедрении цифровых паспортов, которые будут позволять взаимодействовать с любыми учреждениями удаленно.

В России в качестве базы для функционирования системы удаленной идентификации служит Единая биометрическая система (ЕБС) – подсистема Единой системы идентификации и аутентификации (ЕСИА), которая запущена на территории РФ в 2018 году. Такие способы идентификации пользователей позволяют расширить степень защищенности персональных данных, а также самих цифровых аккаунтов, которые используются для получения финансовых услуг. Сейчас система ЕБС поддерживают более 150 российских банков, включая Сбербанк, ВТБ, Тинькофф, Почта-банк, «Хоум кредит» и др. Биометрические данные хранятся в зашифрованном и защищенном виде в хранилище «Ростелекома» в соответствии с требованиями Федерального закона №152-ФЗ «О персональных данных» [4]. Оператор предоставляет для удаленной идентификации граждан мобильное приложение «Ключ Ростелеком». При создании шлюза для идентификации каждый банк может выбрать «Ключ Ростелеком» в качестве базовой платформы или создать собственное приложение с другой технологией.

Одновременно с ЕБС в России существует и НСУД – национальная система управления данными, которая включает в себя информацию о каждом гражданине страны и организации, действующей на территории государства. При этом многими исследователями отмечается, что эта база данных впоследствии будет использоваться в качестве основы не только идентификации в финансовых приложениях, но и для использования цифрового паспорта [8].

Таким образом, современная индустрия финтех использует большой перечень персональных данных клиентов – от стандартных паспортных данных, до биометрии. При этом, если углубляться в особенности российского законодательства, то становится очевидным, что в перспективе российские нормативные правовые акты не могут обеспечить совершенные механизмы защиты этих данных от кибератак, мошенничества и др. На сегодняшний день большую роль в регулировании этого вопроса выполняют различные рекомендации и стандарты Банка России, например Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2020, в котором закрепляются особенности процедуры идентификации и аутентификации в программных приложениях с использованием технологий OpenID [9]. То есть особенности элементов защиты персональных данных больше рассматриваются с точки зрения особенностей и инноваций программного обеспечения. Однако здесь, по моему мнению, необходимо параллельное закрепление ответственности и общих стандартов или технологий, которые необходимы для предоставления финансовых услуг клиентам.

Самим Банком России отмечается необходимость следующих мероприятий для поддержания безопасности использования финтех технологий [10]:

1. Совершенствование комплекса отраслевых стандартов и правил, устанавливающих требования к обеспечению технологической устойчивости, бесперебойности и безопасности при применении финтех, и нормативное закрепление обязанности по их применению;
2. Разработка новых форм и методов взаимодействия и реагирования на информационные

угрозы;

3. Проведение комплекса мероприятий по повышению технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, а также мониторингу состояния информационных систем финансовых организаций.

Таким образом, основная необходимость современного правового регулирования защиты персональных данных при использовании финансовых технологий заключается в повышении уровня технологической безопасности (самих систем, баз данных, специальных приложений для получения клиентами финансовых услуг), обеспечения устойчивости и стабильности финтех, а также повышение уровня взаимодействия между участниками рынка предоставления финансовых услуг с Банком России в целях предупреждения киберпреступлений, которые в том числе связаны с персональными данными пользователей. Для достижения этих целей необходимо внесение изменений в российское законодательство, которое бы затрагивало особенности предоставления финансовых услуг населению удаленно.

Список литературы:

1. Перцева С. Ю. Финтех-индустрия и информационная безопасность // С. Ю. Перцева // Мировое и национальное хозяйство. – № 4 (46). – 2018. – с. 1-5.
2. Федеральный закон от 20.07.2020 № 211-ФЗ «О совершении финансовых сделок с использованием финансовой платформы» // Собрание законодательства РФ. – 27.07.2020. – № 30. – ст. 4737.
3. Развитие финансовых технологий // Центральный банк Российской Федерации. Финтех: сайт. 2021. URL: <https://cbr.ru/fintech/> (дата обращения: 25.12.2021).
4. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // Собрание законодательства РФ. – 31.07.2006. – № 31 (1 ч). – ст. 3451.
5. Солдатова В. И. Защита персональных данных в условиях применения цифровых технологий / В. И. Солдатова // Lex Russica. – 2020. – №2 (159).
6. Rs 500, 10 minutes, and you have access to billion Aadhaar details // The Tribune: сайт. 2018. URL: <https://www.tribuneindia.com/news/archive/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details-523361> (дата обращения: 25.12.2021).
7. Apple Card // Apple. Apple Card: сайт. 2020. URL: <https://www.apple.com/apple-card/> (дата обращения: 25.12.2021).
8. Клиентская аутентификация в финтехе: практика и перспективы // Завтра облачно. Бизнес: сайт. 2020. URL: <https://mcs.mail.ru/blog/personalnaya-autentifikacia-v-rossii> (дата обращения: 25.12.2021).
9. Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2020 “Безопасность финансовых (банковских) операций Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OPENID Требования Financial-grade API Security. Requirements // СПС «Гарант». Информационно-техническое обеспечение: сайт. 2020. URL: <https://www.garant.ru/products/ipo/prime/doc/74706070/> (дата обращения: 25.12.2021).
10. Основные направления развития финансовых технологий на период 2018-2020 годов // Центральный банк Российской Федерации. Финтех: сайт. 2018. URL: https://cbr.ru/Content/Document/File/85540/ON_FinTex_2017.pdf (дата обращения: 25.12.2021).