

Научная статья

УДК 347.121

DOI 10.25205/2542-0410-2023-19-3-23-29

Проблемы защиты персональных данных в банковской сфере

Елена Васильевна Горячева

Сибирский институт управления – филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации

Новосибирск, Россия

goryacheva-ev@ranepa.ru

Аннотация

Актуальность проблем защиты персональных данных приобретает в последнее время особое значение в силу стремительного внедрения цифровизации в мировую и национальные экономики, в том числе цифровые технологии приобретают все большее влияние и в финансово-банковской сфере. В статье рассматриваются проблемы защиты персональных данных в банковских отношениях, анализируются тесно взаимосвязанные понятия «персональные данные» и «банковская тайна». Автором отмечается необходимость совершенствования процесса защиты персональных данных, дальнейшего развития законодательства и выработки жестких стандартов обеспечения безопасности персональных данных клиентов банка. Приведены примеры законодательного опыта Китайской Народной Республики в области защиты персональных данных.

Ключевые слова

персональные данные, банковская тайна, безопасность личных данных, ответственность

Для цитирования

Горячева Е. В. Проблемы защиты персональных данных в банковской сфере // Юридическая наука и практика. 2023. Т. 19, № 3. С. 23–29. DOI 10.25205/2542-0410-2023-19-3-23-29

Problems of Personal Data Protection in the Banking Sector

Elena V. Goryacheva

Siberian Institute of Management – Branch of the Russian Academy of National Economy
and Public Administration under the President of the Russian Federation

Novosibirsk, Russia

goryacheva-ev@ranepa.ru

Annotation

The urgency of the problems of personal data protection has recently acquired particular importance due to the rapid introduction of digitalization into the global and national economies, including digital technologies are gaining increasing influence in the financial and banking sector. The article discusses the problems of personal data protection in banking relations, analyzes the closely interrelated concepts of “personal data” and “banking secrecy”. The author notes the need to improve the process of personal data protection, further development of legislation and the development of strict standards for ensuring the security of personal data of bank customers. Examples of the legislative experience of the People’s Republic of China in the field of personal data protection are given.

Keywords

personal data, banking secrecy, personal data security, responsibility

© Горячева Е. В., 2023

For citation

Goryacheva E. V. Problems of personal data protection in the banking sector. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 23–29. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-23-29

Институт защиты персональных данных является важным элементом механизма защиты прав и свобод граждан, представляющих наивысшую ценность любого правового государства. Состояние защищенности личности достигается комплексом мер, включающих формирование законодательной основы, устанавливающей общие принципы обеспечения безопасности оборота персональных данных и надзора в области прав субъектов персональных данных. Кроме того, специфика правового регулирования зависит от направления деятельности оператора персональных данных, например, в банковской сфере.

В 2006 г. был принят Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Закон о персональных данных), регулирующий отношения, связанные с обработкой персональных данных с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации¹. История поправок в Закон о персональных данных наглядно показывает сложность и актуальность регулируемых им отношений. В редакцию норм Закона о персональных данных правки вносились 27 федеральными законами, но стремительное развитие цифровых технологий свидетельствует о необходимости дальнейшего совершенствования законодательства о защите персональной информации.

Основным понятием в области законодательства о защите персональных данных является понятие персональных данных. Статья 3 Закона о персональных данных определяет персональные данные в качестве любой информации, относящейся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). В силу того, что законодателем использован широкий подход к рассматриваемому определению, в судебной практике возникают споры о характере и объеме сведений, которые необходимо отнести к персональным данным.

Дискуссии относительно содержания понятия персональных данных продолжаются и в научной литературе. При этом авторы едины во мнении, что неоднородность понятия персональных данных создает основу для разночтений в правоприменительной практике. Следует отметить, что научные работы, посвященные обозначенной проблематике, публикуются с момента принятия Закона о персональных данных и в течение всего периода его действия, что свидетельствует о сохраняющей актуальность проблеме [1, с. 44; 2, с. 50].

Поскольку формулировка недостаточно определена под категорию персональных данных, на сегодняшний день подпадают разные по своей природе разновидности личной информации: имя, отчество, фамилия гражданина, его изображение, уникальные идентификационные номера (ИНН, СНИЛС), конфиденциальные личные сведения (сведения о его здоровье, детях, социальном страховании, домашний адрес).

В 2020 г. в Законе о персональных данных было закреплено понятие персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном федеральным законом. Банки могут передавать персональные данные клиентов только с их согласия, которое должно быть конкретным, предметным, информированным, сознательным и однозначным.

¹ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006.

Обработка данных в Законе о персональных данных также толкуется очень широко, поскольку охватывает любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

С точки зрения формулировки, гражданин, предоставивший согласие на обработку, дает согласие на распространение этих данных определенному кругу лиц.

При этом в силу императивных законодательных предписаний как клиент, обратившийся в банк для получения какого-либо банковского продукта, фактически вынужден предоставить согласие на обработку персональных данных, так и банк обязан передавать сведения о клиенте государственным органам, поскольку и эта обязанность на кредитные организации возложена законом.

Пределы раскрытия банковской тайны (порядок и условия предоставления указанной информации) без согласия владельцев счетов определяются ст. 26 Федерального закона «О банках и банковской деятельности» от 02.12.1990 № 395-1 (далее – Закон о банках)². Справки по операциям и счетам клиентов выдаются кредитной организацией им самим, судам и арбитражным судам (судьям), Счетной палате Российской Федерации, налоговым органам, Пенсионному фонду Российской Федерации, Фонду социального страхования Российской Федерации и органам принудительного исполнения судебных актов. Информацию, составляющую банковскую тайну, вправе получать от банков также Агентство по страхованию вкладов, кредитное бюро, Росфинмониторинг, таможенные органы и др.

Общее правило ответственности банка за разглашение банковской тайны и персональных сведений таково, что за разглашение сведений служащими отвечает банк. Кроме того, возможна и ответственность банка по обязательствам из причинения вреда, если вред причинен разглашением сведений о клиенте.

В сфере правового регулирования банковских отношений существует вопрос соотношения тесно взаимосвязанных режимов банковской тайны и персональных данных.

Имеющееся в законодательстве несовпадение в составе сведений, на которые распространяется режим охраны банковской тайны, которое заключается в различии легального определения банковской тайны в ст. 857 ГК РФ и ст. 26 Закона о банках, осложняется широким определением персональных данных, содержащимся в специальном законодательстве.

Согласно п. 1 ст. 857 ГК РФ банк гарантирует тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте.

В силу ст. 26 Закона о банках кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов. Все служащие кредитной организации обязаны хранить тайну об операциях, о счетах и вкладах ее клиентов и корреспондентов, а также об иных сведениях, устанавливаемых кредитной организацией, если это не противоречит федеральному закону.

Формулировка, которой оперирует ГК РФ в части обязанности банка гарантировать тайну сведений о клиенте, позволит нам говорить, что в гражданском законодательстве используется более широкое понимание термина «банковская тайна». При этом норма п. 1 ст. 857 ГК РФ также не определяет точную комбинацию данных о клиенте, что влечет возникновение вопроса о характере сведений, сохранность которых банк обязан гарантировать. По своему содержанию понятие сведений о клиенте непосредственно перекликается со сферой персональных данных.

² Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // Ведомости съезда народных депутатов РСФСР от 6 декабря 1990 г. № 27. Ст. 357.

Достаточно широкие дефиниции персональных данных в Законе о персональных данных и сведений о клиенте, предусмотренных в ГК РФ, не создают основы для позитивной практики правоприменения. При этом нарушения в области обеспечения сохранности персональных данных, их конфиденциальности и законности передачи данных клиентов банков третьим лицам являются наиболее распространенными в банковском секторе.

В последние годы многие клиенты банков пострадали от действий мошенников, которые по телефону обманным путем вынуждали граждан переводить деньги со своих счетов. Поскольку преступниками использовался минимальный объем информации о гражданине (фамилия, имя, отчество и номер телефона), вероятно, утечка персональной информации произошла не из кредитных организаций, поскольку они владеют значительно большим объемом сведений о своих клиентах.

При этом в практике есть примеры, когда информация к мошенникам попадает именно от сотрудников банков. Судебная практика по данной категории дел разнится и в некоторых делах оспаривание действий банка для клиента представляет значительную сложность. Так, Судебная коллегия по гражданским делам Верховного суда Российской Федерации рассмотрела дело по иску Рыбникова к ПАО «Сбербанк» о признании незаключенным договора банковского обслуживания, на основании которого на имя истца был открыт счет, возложении обязанности отозвать соответствующие сведения из базы Федеральной налоговой службы России, компенсации морального вреда и взыскании судебных расходов³.

Названные требования Рыбников мотивировал тем, что по сведениям Федеральной налоговой службы на его имя открыты счета в разных отделениях банка, в том числе в филиале ответчика в Волго-Вятском банке. Истец, ссылаясь на то, что банковский счет с использованием его персональных данных открыт незаконно, также обращал внимание на тот факт, что с использованием этого счета осуществлялись многочисленные операции с денежными средствами, о которых ему ничего неизвестно.

Решением Вахитовского районного суда г. Казани Республики Татарстан, оставленным без изменения апелляционным определением судебной коллегии по гражданским делам Верховного Суда Республики Татарстан и определением судебной коллегии по гражданским делам Шестого кассационного суда общей юрисдикции, исковые требования оставлены без удовлетворения.

В результате только Судебная коллегия по гражданским делам Верховного суда Российской Федерации нашла жалобу гражданина подлежащей удовлетворению. Коллегия отметила, что нижестоящими инстанциями не были приняты во внимание достаточно веские доводы истца, о том, что карта произведена без его ведома и участия, по карте зафиксированы многочисленные расходные операции и операции по зачислению. В период действия карты Рыбников проживал и работал в другом городе (1 300 км от города, где была открыта карта), в трудовых отношениях с организацией, оформившей карту в рамках зарплатного договора, никогда не состоял. Примечательно, что в материалах судебного дела содержалось письмо Рыбникову от начальника сектора Центра заботы о клиентах ПАО «Сбербанк», где обращается внимание на то, что в отношении истца, вероятно, совершены мошеннические действия со стороны третьих лиц, однако установить причастность сотрудников банка к данной ситуации не представляется возможным по причине давности события.

Несмотря на аргументированную и документально подтвержденную позицию истца, нижестоящие суды отказали в удовлетворении исковых требований. Ситуация иллюстрирует сложность доказывания в гражданском процессе факта утечки из банка информации, составляющей банковскую тайну или персональные данные клиента. В этой связи представляется

³ Определение Судебной коллегии по гражданским делам Верховного суда Российской Федерации от 16 февраля 2021 г. № 11-КГ20-18-К6. URL: <https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=ARB&n=65> (дата обращения: 12.05.2023).

необходимым совершенствование в российском законодательстве механизма ответственности за разглашение персональной информации.

В условиях цифровизации экономики перспективным решением проблемы защиты персональных данных клиентов банка представляется использование биометрии для аутентификации клиентов. Традиционные банковские услуги сегодня перемещаются на цифровую платформу и возникает необходимость совершенствования процесса подтверждения личности клиента банка в условиях цифровизации.

Мировая практика правового регулирования и защиты персональных данных достаточно молода. Лидирующие позиции в цифровизации экономики занимает Китайская Народная Республика, чей опыт правового регулирования защиты персональных данных может быть полезен для России.

Нормативно-правовыми актами в сфере защиты данных в этой стране являются Гражданский Кодекс Китайской Народной Республики, вступивший в силу 1 января 2021 года (далее – ГК КНР) [3], Закон Китайской Народной Республики о безопасности данных, вступивший в силу 1 сентября 2021 года (далее – Закон КНР о безопасности данных) [4], Закон Китайской Народной Республики о защите персональной информации, вступивший в силу 1 ноября 2021 года (далее – Закон КНР о защите персональной информации) [5].

В статье 1034 ГК КНР дано понятие личной информации, которой признается информация, записанная в электронном виде или другими способами, которая может использоваться сама по себе или в сочетании с другой информацией для идентификации физического лица, включая имя, дату рождения, идентификационный номер, биометрическую информацию, адрес проживания, номер телефона, адрес электронной почты, медицинскую информацию, местонахождение человека и пр. К частной личной информации применяются положения о праве на неприкосновенность частной жизни или в случае отсутствия которых положения о защите личной информации.

Законом КНР о безопасности данных предусмотрена система мер по обеспечению надзора за безопасностью данных и регулированию деятельности, связанной с обработкой данных. В этой сфере для российской практики представляются интересными ряд норм Закона КНР о безопасности данных, например, в ст. 13 предусмотрена обязанность государства по разработке общего плана координации и безопасности использования данных. В ст. 39 Закона КНР о безопасности данных на государственные органы возложена обязанность создавать надежные системы управления безопасностью данных, выполнять обязанности по защите данных и обеспечивать безопасность правительственных данных.

Важно отметить, что в главе VI «Ответственность» за разглашение охраняемых сведений предусмотрены достаточно высокие общие штрафы для физических лиц и организации от 50 000 до 500 000 юаней (соответственно от 500 000 до 5 500 000 рублей). Если же разглашение сведений ставит под угрозу национальный суверенитет, сумма штрафа составляет от 2 000 000 до 10 000 000 юаней (от 22 240 000 до 111 200 000 рублей).

Помимо штрафов, предусмотрена конфискация доходов посредника по операциям с данными, отдельные виды штрафов за отказ сотрудничать с государственными учреждениями, уполномоченными осуществлять надзор за безопасностью данных. Отдельно предусмотрена прямая личная ответственность должностных лиц за ненадлежащее выполнение должностных обязанностей, злоупотребление властью с целью личной выгоды.

Главой VII Закона КНР о защите персональной информации предусмотрены следующие меры ответственности: предписание об устранении нарушения, конфискация доходов, предписание о приостановлении деятельности, штраф до 1 000 000 юаней (11 120 000 рублей), в случае невыполнения предписания штраф на лиц с прямой ответственностью от 10 000 до 100 000 юаней (от 111 200 до 1 112 000 рублей).

Практика применения высоких штрафов в большинстве случаев не поддерживается российским законодателем. Для сравнения в российском КоАП за обработку персональных дан-

ных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработку персональных данных, несовместимую с целями сбора персональных данных, предусмотрен административный штраф на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц – от десяти тысяч до двадцати тысяч рублей; на юридических лиц – от шестидесяти тысяч до ста тысяч рублей (п. 1 ст. 13.11 КоАП РФ)⁴.

Однако внедрение некоторых из используемых в китайском законодательстве видов ответственности в российскую правовую систему представляется целесообразным, поскольку сегодня отечественным законодателем избраны относительно мягкие виды ответственности, что не способствует эффективной защите охраняемых законодательством отношений.

Отдельного внимания заслуживает роль финансового регулятора (Народного банка Китая) в установлении стандартов защиты персональных данных.

Э. В. Горян рассматривает особенности обеспечения персональных данных в финансово-банковской сфере Китая и приводит стандарты в финансовой сфере, принятые в 2020 г. [6, с. 22]. Во-первых, в Китае действует Техническая спецификация защиты личной финансовой информации, которая определяет уровни и категории личной финансовой информации. Во-вторых, Руководство по классификации безопасности данных требует разграничения уровней безопасности от высокого до низкого с учетом воздействия на национальную безопасность, общедоступность. В-третьих, в Китае существует специальный документ по защите прав и интересов потребителей финансовых услуг [6, с. 27].

Таким образом, опыт Китайской Народной Республики свидетельствует о формировании специального нормативного регулирования защиты личной информации в банковской сфере и ужесточении требований к финансовым операторам. Данная практика представляется перспективной и для российской правовой системы.

Список литературы

1. **Алямкин С. Н.** Персональные данные как объект правового регулирования: понятие и способы защиты // Мир науки и образования. 2016. № 4. С. 44–48
2. **Гнедков А. В., Нищик А. В.** Особенности распространения персональных данных в последней редакции законодательства о персональных данных // Научно-методическое обеспечение оценки качества образования. 2022. № 1 (15). С. 49–52.
3. Гражданский Кодекс Китайской Народной Республики, вступивший в силу 1 января 2021 года [Электронный ресурс]. URL: <https://ru.chinajusticeobserver.com/law/x/civil-code-of-china-part-iv-personality-rights-20200528>
4. Закон Китайской Народной Республики о безопасности данных, вступивший в силу 1 сентября 2021 года [Электронный ресурс]. URL: <https://ru.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610>
5. Закон Китайской Народной Республики о защите персональной информации, вступивший в силу 1 ноября 2021 года [Электронный ресурс]. URL: <https://ru.chinajusticeobserver.com/law/x/personal-information-protection-law20210820>
6. **Горян Э. В.** Безопасность персональных данных в КНР: тенденции совершенствования правового регулирования в финансово-банковском секторе // Административное и муниципальное право. 2021. № 5. С. 15–32.

References

1. **Alamkin S. N.** Personal data as an object of legal regulation: concept and ways of protection // The World of Science and Education, 2016. No. 4. P. 44–48. (in Russ.)

⁴ Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ // Российская газета. 31.12.2001. № 256.

2. **Gnedkov A. V., Nischik A. V.** Features of personal data dissemination in the latest version of the legislation on personal data // Scientific and methodological support of education quality assessment. 2022. № 1 (15). P. 49–52. (in Russ.)
3. Civil Code of the People's Republic of China, effective 1 January 2021. URL: <https://ru.chinajusticeobserver.com/law/x/civil-code-of-china-part-iv-personality-rights-20200528>
4. Data Security Law of the People's Republic of China, effective 1 September 2021. URL: <https://ru.chinajusticeobserver.com/law/x/data-security-law-of-the-people-s-republic-of-china20210610>
5. Personal Information Protection Law of the People's Republic of China, effective 1 November 2021. URL: <https://ru.chinajusticeobserver.com/law/x/personal-information-protection-law20210820>
6. **Goryan E. V.** Security of personal data in the PRC: trends in improving legal regulation in the financial and banking sector // Administrative and Municipal Law. 2021. № 5. P. 15–32. (in Russ.)

Информация об авторе

Елена Васильевна Горячева, кандидат юридических наук

Information about the Author

Elena V. Goryacheva, PhD in Law

Статья поступила в редакцию 14.05.2023;

одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 14.05.2023;

approved after reviewing 21.06.2023; accepted for publication 31.07.2023