ЮРИДИЧЕСКАЯ НАУКА И ПРАКТИКА

Научный журнал
Основан в ноябре 1999 года

2023. Том 19, № 3

СОДЕРЖАНИЕ

ISSN 2542-0410
Юридическая наука и практика. 2023. Т. 19, № 3
Juridical Science and Practice, 2023, vol. 19, no. 3

ISSN 2542-0410
Юридическая наука и практика. 2023. Т. 19, № 3
Juridical Science and Practice, 2023, vol. 19, no. 3

JURIDICAL SCIENCE AND PRACTICE

Scientific Journal
Since 1999, November
In Russan

2023. Volume 19, № 3

CONTENTS

ISSN 2542-0410
Юридическая наука и практика. 2023. Т. 19, № 3
Juridical Science and Practice, 2023, vol. 19, no. 3

The journal is published quarterly in Russian since 1999
by Novosibirsk State University Press

The address for correspondence
Law Department, Novosibirsk State University
1 Pirogov Street, Novosibirsk, 630090, Russian Federation
Tel. +7 (383) 363 42 54

E-mail address: pravo@vestnik.nsu.ru; urfakngu@yandex.ru

On-line version: http://elibrary.ru

УДК 340
DOI 10.25205/2542-0410-2023-19-3-5-8

Итоги проведения круглого стола «Актуальные проблемы защиты персональных данных и кибербезопасность в цифровую эпоху»

Надежда Юльевна Чернусь

Новосибирский национальный исследовательский государственный университет
Новосибирск, Россия

preiudicia@yandex.ru, https://orcid.org/0000-0001-9316-524X

Аннотация

13 апреля 2023 г. в Институте философии и права Новосибирского национального исследовательского государственного университета состоялся круглый стол «Актуальные проблемы защиты персональных данных и кибербезопасность в цифровую эпоху». В его работе приняли участие представители ведущих высших учебных заведений Сибири. На круглом столе был рассмотрен широкий круг проблем, связанный со сложностями толкования и применения законодательства о защите персональных данных, обеспечением безопасности в киберпространстве. Особое внимание было уделено влиянию на эти процессы современных достижений науки и техники, а также широкого использования цифровых технологий.

Ключевые слова

персональные данные, защита персональных данных, кибербезопасность, цифровое пространство, цифровой профиль личности

Для цитирования

Чернусь Н. Ю. Итоги проведения круглого стола «Актуальные проблемы защиты персональных данных и кибербезопасность в цифровую эпоху» // Юридическая наука и практика. 2023. Т. 19, № 3. С. 5–8. DOI 10.25205/2542-0410-2023-19-3-5-8

Actual Problems of Personal Data Protection and Cybersecurity in the Digital Age (Round Table)

Nadezhda Yu. Chernus

Novosibirsk National Research State University
preiudicia@yandex.ru, https://orcid.org/0000-0001-9316-524X

Abstract

On April 13, 2023, the Institute of Philosophy and Law of Novosibirsk National Research State University hosted a round table “Current problems of personal data protection and cybersecurity in the digital age”. Representatives of the leading higher educational institutions of Siberia took part in its work. The round table discussed a wide range of issues related to the difficulties of interpretation and application of legislation on the protection of personal data, ensuring security in cyberspace. Special attention was paid to the influence of modern achievements of science and technology on these processes, as well as the widespread use of digital technologies.

Keywords

personal data, personal data protection, cybersecurity, digital space, digital identity profile

For citation

Chernus N. Yu. Actual problems of personal data protection and cybersecurity in the digital age (Round table). *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 5–8. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-5-8

Представленный Вашему вниманию номер журнала «Юридическая наука и практика» объединил на своих страницах статьи, посвященные одной тематике: проблемам, которые были предметом обсуждения 13 апреля 2023 г. в Институте философии и права Новосибирского национального исследовательского государственного университета на круглом столе «Актуальные проблемы защиты персональных данных и кибербезопасность в цифровую эпоху». В его работе приняли участие представители ведущих высших учебных заведений Сибири. На круглом столе был рассмотрен широкий круг проблем, связанный со сложностями толкования и применения законодательства о защите персональных данных, обеспечением безопасности в киберпространстве. Особое внимание было уделено влиянию на эти процессы современных достижений науки и техники, а также широкого использования цифровых технологий. Тематический выпуск журнала содержит статьи участников круглого стола, посвященные актуальным проблемам защиты персональных и обеспечению кибербезопасности.

С приветственным словом к участникам круглого стола обратился **директор Института философии и права НГУ, доктор философских наук, профессор Владимир Серафимович Диев**. Он подчеркнул, что защита персональных данных стала одной из актуальных проблем для исследования в различных отраслях науки. Отметил, что в XXI в. человек осознает гарантированность своих прав и их незыблемость, поскольку результатом общественного прогресса стали расширение количества основных прав и свобод человека и конкретизация их содержания, признание прав человека на международном уровне, возложение на государство обязанностей по их обеспечению и защите. Программа круглого стола, по его мнению, позволяет рассмотреть проблематику защиты персональных данных сквозь призму взаимодействия национальных ценностей, специфики правового регулирования данных отношений различными отраслями права, развития новых технологий. Конструктивная работа участников круглого стола придаст новый импульс дальнейшему развитию теории и практики защиты персональных данных.

Заместитель директора Института философии и права НГУ, доктор юридических наук, доцент Николай Иванович Красняков в своем приветственном слове обратил внимание, что проблема защиты персональных данных заключается в том, что информатизация и развитие виртуального пространства способствуют порождению новых отношений, требующих законодательного регулирования и, возможно, изменения действующего законодательства. Согласно Конституции РФ, каждый человек имеет право на неприкосновенность частной жизни, защиту своей чести и доброго имени. Сбор, хранение и распространение персональных данных лица без его согласия запрещается (ст. 23 Конституции РФ). Защита частной жизни и обеспечение ее неприкосновенности – это та область, в охране которой заинтересован каждый человек и государство. В этой связи обратил внимание на необходимость разработки новой концепции, обеспечивающей баланс общего блага и личных интересов граждан в условиях глобальной цифровизации всех сфер жизнедеятельности.

В своем выступлении **доктор юридических наук, профессор кафедры уголовного права, уголовного процесса и криминалистики Института философии и права Новосибирского государственного университета Роман Николаевич Боровских** раскрыл уголовно-правовые аспекты кибербезопасности на основе анализа отчета ГИАЦ МВД России, выделил две группы преступлений в сфере информационных технологий: первая – преступления, совершенные с использованием информационно-телекоммуникационных технологий; вторая – преступления в сфере компьютерной информации. В докладе Р. Н. Боровских проанализировал виды преступлений в сфере кибербезопасности.

Проблему обеспечения конфиденциальности персональных данных в ситуации киберугроз затронула **кандидат юридических наук, доцент кафедры предпринимательского права, гражданского и арбитражного процесса Института философии и права Новосибирского государственного университета Елизавета Владимировна Зайнутдинова.** Он отметила, что несмотря на наличие в законодательстве требований к обработке персональных данных

и их оборота в сети «Интернет», нередки случаи утечки персональных данных. Необходимо обеспечить защиту персональных данных в цифровой среде ввиду возможных кибератак и отсутствия надлежащих мер и гарантий в указанной сфере. Был предложен авторский подход к совершенствованию законодательства о защите персональных данных, который заключается в проведении проверки деятельности оператора на предмет нарушений, приведших к утечке персональных данных (постконтроль), во внедрении комплаенс-системы, позволяющей превентивно предотвращать утечки и иные нарушения в сфере персональных данных (априоритроль), а также обучение сотрудников для минимизации рисков разглашения и иного незаконного использования персональной информации.

Доцент кафедры гражданского права Юридического института Алтайского государственного университета, кандидат юридических наук Дмитрий Валерьевич Пятков посвятил свое выступление способам получения согласия субъекта персональных данных на их обработку в процессе организации образовательных онлайн-курсов. На примере своей педагогической практики раскрыл особенности получения и оформления согласия субъекта персональных данных на обработку персональных данных в ситуации дистанционного обучения. На основе анализа действующего законодательства о защите персональных данных сформулировал вывод о том, что согласие на обработку персональных данных может быть получено с использованием электронных средств коммуникации и передачи данных, таких как электронная почта, сервис «Yandex Forms» и др.

Доклад кандидата юридических наук, доцента кафедры гражданского права и процесса Сибирского института управления Российской академии народного хозяйства и государственной службы Елены Анатольевны Дорожинской посвящен актуальным проблемам построения внутрикорпоративной системы комплаенса в области защиты персональных данных. В выступлении проанализированы положения законодательства, направленные на организацию внутрикорпоративной системы комплаенса в области защиты персональных данных. Продемонстрирована корпоративная и судебная практика, отражающая изменение правового регулирования комплаенса организаций в сфере сбора и использования персональных данных. Автор сформулировал рекомендации по разработке внутренних документов корпорации, регламентирующих обработку персональных данных корпорации.

В своем выступлении **кандидат юридических наук, младший научный сотрудник отдела социальных и правовых исследований Института философии и права СО РАН Анастасия Николаевна Артемова** обратилась к особенностям правового регулирования трансграничной передачи персональных данных. Рассмотрела новеллы российского законодательства в области регулирования трансграничной передачи персональных данных, продемонстрировала различия в уведомительном и разрешительном порядках защиты прав субъектов персональных данных. На основе сравнительно-правового исследования был сформулирован вывод о том, что придание российскому закону о персональных данных экстерриториального характера соответствует новейшей тенденции, сложившейся в зарубежных правопорядках.

Кандидат юридических наук, PhD, доцент кафедры гражданского права и процесса Сибирского института управления Российской академии народного хозяйства и государственной службы Елена Васильевна Горячева в своем докладе затронула проблемы защиты персональных данных в банковской сфере.

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. При-

ведены примеры законодательного опыта Китайской Народной Республики в области защиты персональных данных.

С докладом выступил **магистрант магистерской программы «Право интеллектуальной собственности и цифровые технологии» Института философии и права Новосибирского государственного университета Сунь Юйпэн**. Он рассмотрел особенности защиты персональных данных по законодательству КНР. В своем выступлении проанализировал законодательство и судебную практику о защите персональных данных в КНР. Рассмотренные Сунь Юйпэном примеры судебной практики КНР демонстрируют применение законодательства о персональных данных, привлечение нарушителей к гражданско-правовой, уголовной и административной ответственности. Сформулирован вывод о том, что развитие интернет-технологий, технологий искусственного интеллекта, глубокого синтеза порождает множество проблем, связанных с незаконным использованием личной информации о гражданах, что требует постоянного совершенствования законодательства о защите персональных данных.

Статьи участников круглого стола отличаются глубиной и творческим подходом к актуальным проблемам защиты персональных данных и кибербезопасности в цифровую эпоху, представлены в данном, специальном номере журнала, изданным Новосибирским национальным исследовательским государственным университетом «Юридическая наука и практика».

Информация об авторе

Надежда Юльевна Чернусь, кандидат юридических наук

Information about the author

Nadezhda Yu. Chernus, Candidate of Law sciences

Научная статья

УДК 349
DOI 10.25205/2542-0410-2023-19-3-9-16

Правовое регулирование трансграничной передачи персональных данных

Анастасия Николаевна Артемова

Институт философии и права СО РАН
Новосибирск, Россия

artemova-an-1991@yandex.ru

Аннотация

В статье рассматриваются новеллы отечественного законодательства в области регулирования трансграничной передачи персональных данных. Анализируются различия в уведомительном и разрешительном порядках, установленных в зависимости от наличия/отсутствия в соответствующем государстве адекватного уровня защиты прав субъектов персональных данных. На основе сравнительно-правового исследования автор приходит к выводу о том, что придание российскому закону о персональных данных экстерриториального характера соответствует новейшей тенденции, сложившейся в других правопорядках (ЕС, США, Китая).

Ключевые слова

персональные данные, трансграничная передача; субъект персональных данных, оператор персональных данных, адекватный уровень защиты, экстерриториальность, сверхимперативные нормы

Для цитирования

Артемова А. Н. Правовое регулирование трансграничной передачи персональных данных // Юридическая наука и практика. 2023. Т. 19, № 3. С. 9–16. DOI 10.25205/2542-0410-2023-19-3-9-16

Legal Regulation of Cross-Border Personal Data Transfer

Anastasiia N. Artemova

Institute of Philosophy and Law SB RAS
Novosibirsk, Russia

artemova-an-1991@yandex.ru

Annotation

The article discusses the novelties of domestic legislation in the field of regulation of cross-border transfer of personal data. Differences in the notification and authorization procedures established depending on the presence / absence in the relevant state of an adequate level of protection of the rights of personal data subjects are analyzed. On the basis of a comparative legal study, the author comes to the conclusion that giving the Russian law on personal data an extraterritorial character corresponds to the latest trend that has developed in other legal orders (EU, USA, China).

Keywords

personal data, cross-border transfer, subject of personal data, personal data operator, an adequate level of protection, extraterritoriality, overriding rules

For citation

Artemova A. N. Legal regulation of cross-border personal data transfer. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 9–16. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-9-16

Современные технологии в буквальном смысле слова стирают границы между странами, что делает проблему защиты персональных данных (далее – ПД) все более актуальной. Растет количество операторов ПД, осуществляющих трансграничную передачу, т. е. передачу ПД на территорию иностранного государства органу власти иностранного государства, иностранному физическому или юридическому лицу (ст. 3 Федерального закона «О персональных данных» №152 от 27.07.2006 (далее – Закон о ПД).

С необходимостью осуществления трансграничной передачи ПД сталкиваются все хозяйствующие субъекты, которые работают с иностранными контрагентами и передают им персональные данные граждан РФ: турагентства, участники внешнеэкономической деятельности, организации, направляющие своих работников на стажировку за границу и т. д.

Трансграничная передача ПД имеет место и в том случае, когда российские граждане совершают онлайн-покупки на сайтах иностранных продавцов или с использованием маркетплейсов, позволяющих приобретать товары из-за рубежа, а также в случае использования программного обеспечения, размещенного на иностранных серверах.

Серьезную озабоченность вызывает рост случаев утечек персональных данных в результате кибератак. Размещенные в свободном доступе на нелегальных сервисах персональные данные российских физических лиц используются злоумышленниками в преступных целях.

Указанные обстоятельства обусловили принятие в 2022 г. Федерального закона № 266[1], целью которого является повышение уровня правовой защищенности субъектов ПД и совершенствование правового регулирования трансграничной передачи персональных данных.

Изменения затронули как непосредственно порядок осуществления трансграничной передачи ПД, так и определение применимого права при рассмотрении судами споров, вытекающих из отношений по обработке ПД граждан РФ, осуществляемой иностранными физическими или юридическими лицами.

Согласно ч. 1 ст. 12 Закона о ПД трансграничная передача персональных данных осуществляется в соответствии с Законом о ПД и международными договорами Российской Федерации. Россия является участницей Конвенции Совета Европы о защите прав физических лиц при автоматизированной обработке персональных данных 1981 г. (далее – Конвенция)[2], которая установила важнейшие принципы защиты персональных данных (в частности, принцип справедливости и законности при обработке ПД, принцип целевого использования, принцип относимости и соразмерности целям хранения, принцип точности и др.). В целях придания данным принципам юридической силы страны-участницы берут на себя обязанность по принятию необходимых мер в рамках внутреннего законодательства.

Кроме того, Конвенция регулирует порядок оказания взаимной помощи договаривающимися странами по вопросам защиты прав субъектов ПД и порядок осуществления трансграничной передачи ПД. Так, в силу п. 2 ст. 12 Конвенции договаривающиеся стороны не должны запрещать или обусловливать специальным разрешением трансграничную передачу ПД на территорию друг друга. В соответствии с принятыми на себя международно-правовыми обязательствами Россия допускает передачу ПД на территорию стран – участниц Конвенции без каких-либо ограничений. Однако с принятием Федерального закона № 266 трансграничная передача ПД становится полностью подконтрольной Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (далее – Роскомнадзор).

---

[1] Федеральный закон «О внесении изменений в Федеральный закон “О персональных данных”», отдельные законодательные акты Российской Федерации о признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» от 14.07.2022 № 266-ФЗ. [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_421898/ (дата обращения: 19.05.2023).

[2] Федеральный закон «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» от 19.12.2005 № 160-ФЗ [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_57153/ (дата обращения: 19.05.2023).

Если ранее для передачи ПД в страны, участвующие в Конвенции, не требовалось соблюдения какой-либо процедуры, то с 1 марта 2023 г. установлено требование предварительного уведомления Роскомнадзора о намерении оператора осуществить трансграничную передачу ПД. В зависимости от того, в какую страну оператор ПД планирует передавать персональные данные физических лиц, Закон предусматривает два порядка осуществления трансграничной передачи персональных данных: уведомительный и разрешительный.

Для передачи ПД в страны, обеспечивающие адекватную защиту прав субъектов ПД, достаточно уведомить Роскомнадзор. К таким странам относятся страны – участницы Конвенции, а также страны, действующие нормы права которых соответствуют положениям Конвенции. В таких странах имеется законодательство о персональных данных, за нарушение требований которого предусмотрена система санкций, а также уполномоченный орган по защите прав субъектов ПД. Так, например, важные торговые партнеры России: Беларусь, Казахстан, Индия, Китай – не участвуют в Конвенции, но удовлетворяют вышеуказанным критериям. Перечень, утвержденный Приказом Роскомнадзора № 128 от 05.08.2022, вступивший в силу с 1 марта 2023 г., содержит 89 стран, обеспечивающих адекватную защиту (из них 55 стран – участниц Конвенции). Передача ПД в остальные страны допускается только с разрешения Роскомнадзора (исключение – ситуации, когда трансграничная передача персональных данных необходима для защиты жизни, здоровья, иных жизненно важных интересов субъекта ПД или других лиц).

Деление стран на обеспечивающих адекватный уровень защиты и не обеспечивающих таковой закреплен и в других правопорядках. В частности, Закон Республики Беларусь «О защите персональных данных» № 99-З от 07.05 2021 по общему правилу запрещает трансграничную передачу ПД в государства, не обеспечивающие надлежащий уровень защиты прав субъектов ПД. Перечень государств, обеспечивающих адекватный уровень защиты, определяется уполномоченным органом по защите прав субъектов ПД (в перечень входят страны – участницы Конвенции Совета Европы). Для трансграничной передачи ПД в страны, не участвующие в Конвенции, установлен разрешительный порядок [1, с. 160].

В рамках Европейского союза с 2018 г. действует Общий регламент о защите данных (General Data Protection Regulation – GDPR), пришедший на смену Директиве ЕС о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных 95/46/ЕС от 24.10.1995 и существенно ужесточивший требования к трансграничной передаче ПД.

В соответствии со ст. 45 Регламента трансграничная передача ПД в страны, обеспечивающие адекватный уровень защиты прав субъектов ПД, не требует специального разрешения. Решение о признании государства обеспечивающим адекватную защиту принимает Европейская Комиссия на основании оценки таких факторов, как верховенство прав человека и фундаментальных свобод, наличие в государстве законодательства в области защиты персональных данных, эффективных административных и судебных средств правовой защиты субъектов ПД, существование и эффективное функционирование надзорных органов, оказывающих содействие субъектам ПД в реализации ими своих прав, участие государства в международных договорах в области защиты персональных данных.

При отсутствии такого решения трансграничная передача данных может осуществляться только в том случае, если оператор ПД обеспечивает соответствующие гарантии и при условии, что субъектам ПД доступны эффективные средства правовой защиты (ст. 46 Регламента).

Кроме того, Общий Регламент ЕС допускает передачу ПД в страны, в отношении которых отсутствует решение Европейской Комиссии об адекватности, с согласия самого субъекта ПД и в исключительных случаях, исчерпывающий перечень которых закреплен в статье 49 Регламента[3].

[3] Общий регламент ЕС по защите данных (General Data Protection Regulation – GDPR) [Электронный ресурс]. URL: https://gdpr-text.com/ru/read/recital-23/ (дата обращения: 19.05.2023).

В Китае, где законодательство в области защиты персональных данных активно развивается, в 2021 г. был принят Закон о защите личной информации (Personal Information Protection Law – PIPL), во многом повторяющий положения Общего Регламента ЕС о защите данных (GDPR).

В отношении трансграничной передачи ПД статья 38 Закона КНР о защите личной информации устанавливает, что оператор ПД должен удовлетворять одному из указанных требований: 1) прохождение оценки безопасности уполномоченным органом по защите прав субъектов ПД – национальным департаментом киберпространства; 2) получение сертификата защиты ПД от соответствующего специализированного учреждения в соответствии с положениями, изданными национальным департаментом киберпространства; 3) заключение договора с иностранным оператором ПД по стандартной форме, утвержденной национальным департаментом киберпространства и устанавливающей права и обязанности обеих сторон; 4) соблюдение иных условий, предусмотренных законами и подзаконными актами, а также национальным департаментом киберпространства Китая[4].

Учитывая возрастающую роль интеграционных объединений в развитии международных экономических отношений, для Российской Федерации на данном этапе перспективным видится международное сотрудничество в области защиты прав субъектов ПД в рамках Евразийского экономического союза (ЕАЭС). Так, одним из направлений на пути к формированию единого цифрового пространства ЕАЭС – необходимого условия развития интеграции государств – членов ЕАЭС в условиях развития цифровой экономики – является проработка международного договора об обороте данных в Союзе (в том числе о защите персональных данных)[5]. Как отмечает Н. А. Шебанова, на данный момент имеются все предпосылки для его разработки: внедрение в рамках ЕАЭС интеграционных цифровых платформ, наличие национальных законов о ПД в государствах – членах ЕАЭС (Россия, Армения, Беларусь, Казахстан, Киргизия); осознание объективной необходимости координации усилий для создания нормативной базы, соответствующей потребностям цифровой экономики [2, с. 51].

Особый интерес представляет вопрос об определении применимого права при трансграничной передаче ПД. Поскольку такие отношения осложнены иностранным субъектом, осуществляющим обработку ПД, при рассмотрении спора, вытекающего из договорных отношений, сторонами которых являются российский субъект ПД и иностранный оператор ПД, суду необходимо решить вопрос о применимом праве.

До недавнего времени этот вопрос не был прямо урегулирован в отечественном праве. Учеными предлагалось обращение к коллизионным нормам, содержащимся в разделе VI части 3 ГК РФ: применение права, выбранного сторонами договора (ст. 1210 ГК РФ), а при отсутствии соглашения сторон о выборе права – права оператора ПД (п. 1 ст. 1211 ГК РФ) [3, с. 707].

Федеральным законом № 266 Закон о ПД был дополнен новой нормой: в соответствии с ч. 1.1 ст. 1 к обработке ПД граждан РФ, осуществляемой иностранными юридическими или физическими лицами, применяются положении российского Закона о ПД.

Целью данной новеллы является придание экстерриториального характера отечественному Закону о ПД[6]: теперь иностранные компании, ориентированные на российский рынок, обрабатывающие ПД россиян, обязаны соблюдать требования российского Закона о ПД. Сто-

[4] Закон КНР о защите личной информации (Personal Information Protection Law – PIPL) [Электронный ресурс]. URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (дата обращения: 19.05.2023).

[5] П. 5.4.2 Решения Высшего Евразийского экономического совета от 11.12.2020 №12 «О Стратегических направлениях развития евразийской экономической интеграции до 2025 года» [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_375194/ (дата обращения: 19.05.2023).

[6] Пояснительная записка к проекту федерального закона «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных»// Официальный сайт Государственной Думы РФ [Электронный ресурс]. URL: https://sozd.duma.gov.ru/bill/101234-8 (дата обращения: 19.05.2023).

ит отметить, что ч. 1.1 ст. 1 Закона о ПД является не односторонней коллизионной нормой, отсылающей отечественного правоприменителя к российскому праву, а именно экстерриториальной нормой, распространяющей нормы отечественного закона за пределы государственной территории, возлагающей на иностранные суды обязанность применять такую норму [4, с. 103].

Тренд на придание национальному законодательству экстерриториального характера был задан Общим Регламентом ЕС по защите данных (GDPR), который распространяет на операторов ПД независимо от места их регистрации обязанность соблюдать его требования в отношении обработки ПД лиц, находящихся на территории стран ЕС.

Критерием применения GDPR является направленность деятельности компании на субъектов ПД из стран ЕС, когда операторы ПД (например, интернет-магазины, хостелы, сайты знакомств, социальные сети и т. д.) предлагают свои товары/услуги субъектам ПД, находящимся в ЕС (используя в этих целях язык, валюту одного или нескольких государств – членов ЕС, предусматривая возможность осуществления заказа товара/услуги на этом языке, упоминая пользователей из стран ЕС), или осуществляют мониторинг их поведенческой активности, имеющей место в ЕС[7].

Впоследствии положения об экстерриториальном характере были закреплены в законах о персональных данных и в других странах, в частности в США и Китае.

Так, например, закон штата Калифорния о конфиденциальности данных потребителей (California Consumer Privacy Act), вступивший в силу в 2020 г., распространяет свое действие на компании, не имеющие физического присутствия в Калифорнии, но ведущие бизнес в этом штате (в том числе посредством сети «Интернет») и собирающие персональные данные жителей Калифорнии, при условии соответствия их выручки пороговому значению [5, с. 66–67].

Закон КНР о защите личной информации (PIPL) в статье 3 предусматривает, что его нормы применяются в отношении иностранных операторов ПД, если они обрабатывают ПД физических лиц, находящихся на территории Китая, в целях предложения им товаров и услуг, а также в случае осуществления анализа их поведенческой активности на территории КНР. Таким образом, данные положения полностью повторяют нормы статьи 3 Регламента ЕС. Однако перечень оснований применения китайского закона не является закрытым. Пункт 3 данной статьи называет также иные обстоятельства, предусмотренные законами или подзаконными актами[8], что оставляет широкую свободу усмотрения для китайских властей и позволяет ученым говорить о высоком уровне правовой неопределенности в этой сфере[9].

Таким образом, придание экстерриториального характера российскому закону не просто отвечает важнейшей цели государства по защите прав своих граждан, но и соответствует последней тенденции развития законодательства о персональных данных в других странах. В условиях глобализации и формирования единого киберпространства рост экстерриториального регулирования становится неизбежным [6, с. 12–13]. Признание за иностранным законом экстерриториального характера способствует налаживанию эффективного сотрудничества государств в правовой сфере, выработке общих межгосударственных решений [7, с. 376].

Вместе с тем придание экстерриториального характера национальному законодательству государства в области защиты персональных данных сопряжено с трудностями как теоретического, так и практического характера. С точки зрения доктрины международного частного

---

[7] Статья 3 Общего регламента ЕС по защите данных (General Data Protection Regulation – GDPR) [Электронный ресурс]. URL: https://gdpr-text.com/ru/read/recital-23/ (дата обращения: 19.05.2023).

[8] Статья 3 Закона КНР о защите личной информации (Personal Information Protection Law – PIPL) [Электронный ресурс]. URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (дата обращения: 19.05.2023).

[9] Zhu J. The Personal Information Protection Law: China's Version of the GDPR? // Columbia Journal of Transnational Law. 14.02.2022. [Электронный ресурс]. URL: https://www.jtl.columbia.edu/bulletin-blog/the-personal-information-protection-law-chinas-version-of-the-gdpr (дата обращения: 19.05.2023).

права это вступает в противоречие с основополагающим принципом суверенитета государства, из которого вытекает возможность применения государством на своей территории исключительно норм иностранного частного права, поскольку частное право, основанное на принципах диспозитивности, равенства, автономии воли, не связано с политикой государства, и его применение не наносит ущерба суверенитету государства. Хотя институт защиты персональных данных призван обеспечивать право лица на неприкосновенность его частной жизни, законодательство в области обработки персональных данных носит ярко выраженный публично-правовой характер.

Отсюда следует трудность уже практического характера: суды могут отказывать в применении норм иностранного закона о ПД либо в признании и приведении иностранного судебного решения в исполнение.

При рассмотрении спора о нарушении прав субъекта ПД при их трансграничной передаче российский суд будет применять отечественное законодательство о персональных данных – *lex fori* (право страны суда). Однако реальное привлечение иностранного лица, осуществляющего обработку ПД, к ответственности возможно только при наличии международного договора о признании и приведении в исполнение судебных решений, а в отсутствие такого договора – при наличии у данного лица каких-либо активов в Российской Федерации.

В случае же рассмотрения спора за рубежом встанет вопрос о возможности экстерриториального применения российского Закона о ПД. Российскому гражданину необходимо будет представить убедительные доказательства того, что Федеральный закон «О персональных данных» действительно должен применяться в рассматриваемом деле и до каких пределов.

Способом разрешения данной коллизии может быть квалификация норм российского Закона о ПД как иностранных сверхимперативных норм, имеющих тесную связь с отношением.

Под сверхимперативными нормами (нормами непосредственного применения – ст. 1192 ГК РФ) понимаются такие нормы, которые в силу их особого значения применяются к отношениям, осложненным иностранным элементом, независимо от подлежащего применению права. При этом в качестве сверхимперативных норм могут выступать не только частноправовые, но и публично-правовые нормы [8, с. 15].

Применение российского Закона о ПД, таким образом, будет зависеть от того, какую позицию занимает иностранный правопорядок относительно допустимости применения иностранной сверхимперативной нормы. Такая возможность предусмотрена, в частности, нормами европейского международного частного права (п. 3 ст. 9 Регламента ЕС №593/2008 о праве, подлежащем применению к договорным обязательствам (Рим-I) 2008 г.).

Наконец, нельзя не отметить закрепление Федеральным законом № 266 нормы, имеющей важный практический характер – возможности привлечь в качестве солидарных ответчиков оператора ПД и лицо, которому оператор ПД поручил обработку ПД. Так, если российский оператор ПД заключает договор на обработку ПД с иностранным физическим или юридическим лицом, отвечать за нарушения прав субъектов ПД будут оба (ч. 6 ст. 6 Закона о ПД).

Подводя итог рассмотрению правового регулирования трансграничной передачи персональных данных, можно сделать следующие выводы. Необходимость обеспечения эффективной защиты прав субъектов персональных данных обусловливает ужесточение порядка осуществления их трансграничной передачи. Как показывает сравнительно-правовой анализ, общей тенденцией развития законодательства о персональных данных на современном этапе является придание экстерриториального характера нормам национальных законов о персональных данных. Между тем практические трудности, сопряженные с экстерриториальным характером таких норм, ставят на повестку дня необходимость развития международного сотрудничества по вопросу взаимного признания и приведения в исполнение решений по делам о защите прав субъектов персональных данных.

Список литературы

1. **Бутич В. А., Михалева Т. Н.** К вопросу о трансграничной передаче персональных данных из Республики Беларусь // Беларусь в современном мире: Материалы XXI Международной научной конференции, посвященной 101-й годовщине образования Белорусского государственного университета, Минск, 27 октября 2022 года / Редколлегия: Е.А. Достанко (гл. ред.) [и др.]. Минск: Белорусский государственный университет, 2022. С. 159-164.
2. **Шебанова Н. А.** Охрана персональных данных в государствах – членах ЕАЭС // Журнал Суда по интеллектуальным правам. 2021. № 3 (33). С. 42–51.
3. **Канашевский В. А.** Международное частное право: Учебник. М.: Международные отношения, 2016. 1008 с.
4. **Морозов Д. В.** Экстерриториальные нормы и доктрина международного частного права // Журнал российского права. 2011. № 7 (175). С. 98–106.
5. **Восс У. Г.** Трансграничные потоки данных, общий регламент защиты персональных данных и управление данными // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17, № 1. С. 56–95. DOI 10.17323/1996-7845-2022-01-03
6. **Самарин А. А.** Экстерриториальное действие права: Автореф. дис. ... канд. юрид. наук. Н. Новгород, 2016. 32 с.
7. **Шестопал С. С.** Соотношение суверенитета государства и экстерриториальности права в контексте глобализации // Азимут научных исследований: экономика и управление. 2017. Т. 6, № 4(21). С. 375–380.
8. **Данилова А. А.** Нормы непосредственного применения (mandatory rules, lois de police, regles de applicacion immediate) в международном частном праве: Дис. ... канд. юрид. наук. М., 2005. 202 с.

References

1. **Butich V. A., Mikhaleva T. N.** On the issue of cross-border transfer of personal data from the Republic of Belarus // Belarus in the modern world: Proceedings of the XXI International Scientific Conference dedicated to the 101st anniversary of the formation of the Belarusian State University, Minsk, October 27, 2022 / Editorial Board: E.A. Dostanko (editor-in-chief) [and others]. Minsk: Belarusian State University, 2022. P. 159–164.
2. **Shebanova N. A.** Protection of personal data in the member states of the EAEU // Journal of the Court for Intellectual Rights. 2021. № 3 (33). Pp. 42–51.
3. **Kanashevsky V. A.** International private law: textbook. M.: International relations, 2016. 1008 p.
4. **Morozov D. V.** Extraterritorial norms and the doctrine of private international law // Journal of Russian law. 2011. No. 7 (175). P. 98–106.
5. **Voss W. G.** Cross-border data flows, general regulations for the protection of personal data and data management // Bulletin of international organizations: education, science, new economy. 2022. Vol. 17, no. 1. P. 56-95. DOI 10.17323/1996-7845-2022-01-03.
6. **Samarin A. A.** Extraterritorial effect of law. Abstract of dis. N. Novgorod, 2016. 32 p.
7. **Shestopal S. S.** Correlation between state sovereignty and extraterritorial law in the context of globalization // Azimut of Scientific Research: Economics and Management. 2017. Vol. 6, no. 4 (21). Pp. 375–380.
8. **Danilova A. A.** Norms of direct application (mandatory rules, lois de police, regles de applicacion immediate) in private international law. Dis. M., 2005. 202 p.

Информация об авторе

Анастасия Николаевна Артемова, кандидат юридических наук
SPIN 5978-6835

Information about the Author

Anastasiia N. Artemova, PhD in Law
SPIN 5978-6835

Статья поступила в редакцию 25.05.2023;
одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 25.05.2023;
approved after reviewing 21.06.2023; accepted for publication 31.07.2023

Научная статья

УДК 343.3
DOI 10.25205/2542-0410-2023-19-3-17-22

Уголовно-правовые аспекты кибербезопасности

Роман Николаевич Боровских

Новосибирский национальный исследовательский государственный университет
Новосибирск, Россия

borovskih80@yandex.ru

Аннотация

В статье рассматриваются вопросы уголовного законодательства РФ об ответственности за преступления в сфере кибербезопасности. Автором анализируется уголовно-правовое содержание данного термина, его юридические границы. На основе исследования формулируются несколько подходов к решению указанной проблемы.

Ключевые слова

уголовное право, преступления в сфере компьютерной информации, кибербезопасность, киберпреступления

Для цитирования

Боровских Р. Н. Уголовно-правовые аспекты кибербезопасности // Юридическая наука и практика. 2023. Т. 19, № 3. С. 17–22. DOI 10.25205/2542-0410-2023-19-3-17-22

Criminal Legal Aspects of Cybersecurity

Roman N. Borovskikh

Novosibirsk State University
Novosibirsk, Russian Federation

borovskih80@yandex.ru

Abstract

The article deals with the issues of the criminal legislation of the Russian Federation on liability for crimes in the field of cybersecurity. The author analyzes the criminal-legal content of this term, its legal boundaries. Based on the study, several approaches are formulated to solve this problem.

Keywords

criminal law, crimes in the field of computer information, cybersecurity, cybercrime

For citation

Borovskikh R. N. Criminal legal aspects of cybersecurity. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 17–22. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-17-22

По данным официальной уголовной статистики [1, с. 31], в 2022 г. в России зарегистрировано 1 966,8 тыс. преступлений, из которых более четверти (522 тыс.) составили преступления, совершенные с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Важно отметить, что в числе данных преступлений свыше 272 тыс. тяжких и особо тяжких (52 %).

Авторы отчета ГИАЦ МВД России оперируют термином, который включает в себя две группы преступлений: первая – преступления, совершенные с использованием информационно-телекоммуникационных технологий; вторая – преступления в сфере компьютерной информации. При этом обе данные группы, согласно отчету, охватывают широкий спектр уголовно наказуемых деяний, в числе которых:

– кража (ст. 158 УК РФ);

– мошенничество и его разновидности (ст. 159, 159.3, 159.6 УК РФ);

– незаконные организация и проведение азартных игр (ст. 171.2 УК РФ);

– публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ);

– незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ);

– изготовление порнографических материалов (ст. 242, 242.1, 242.2 УК РФ);

– публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ);

– преступления в сфере компьютерной информации (глава 28 УК РФ).

Как видно, к числу «компьютерных» преступлений отнесены преступления различных родов и видов.

Критериями, на основании которых авторы отчета МВД РФ объединили вышеперечисленные преступления в одну группу для статистического измерения, были определены следующие:

– совершение преступления с использованием или применением расчетных (пластиковых) карт (речь идет о средствах совершения преступления);

– использование для преступных целей компьютерной техники, программных средств, фиктивных электронных платежей, сети «Интернет», средств мобильной связи (подразумеваются способы совершения преступлений).

Таким образом, с одной стороны, вышеприведенные сведения определенным образом формируют представление о том, что, по мнению аналитиков МВД РФ, содержательно означают категории «преступление, совершенное с использованием информационно-телекоммуникационных технологий и «преступление в сфере компьютерной информации». Выразим согласие с необходимостью столь широкого подхода в их понимании. Вместе с тем становится понятным, что определенных уголовно-правовых границ первая из рассматриваемых категорий не имеет, равно как и нет четкого понимания ее соотношения со второй категорией, которая формально ограничена главой 28 УК РФ. В связи с этим можно констатировать отсутствие четких дефинитивных границ рассматриваемых групп преступлений (отметим, что понятие «преступление в сфере компьютерной информации», несмотря на указанную одноименную главу, может также иметь более широкую, выходящую за пределы данной главы трактовку; например, когда речь идет о включении в число таких преступлений мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) или ряда иных преступлений).

В научной литературе широко обсуждается вопрос о терминологическом аппарате уголовно-правового противодействия рассматриваемым преступлениям. В числе прочего предлагаются к использованию (в том числе в нормативном аспекте) категории «киберпреступление» или «преступление в сфере кибербезопасности» [2; 3] При этом под киберпреступлениями предлагается понимать любые преступления, которые совершаются в киберпространстве (информационном пространстве) с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных [4, с. 48].

В целом, соглашаясь с возможностью использования в уголовно-правовом лексиконе понятий «киберпреступление» или «преступление в сфере кибербезопасности» (далее будем

рассматривать их равнозначными), попробуем определить критерии, на основании которых конкретное преступление следует относить к числу таковых. Но прежде несколько слов о сочетаемости в уголовно-правовом дискурсе терминов «кибер» и «безопасность».

Во-первых, уголовно-правовой принцип гуманизма предусматривает, что уголовное законодательство России обеспечивает *безопасность* (курсив мой. – *Р. Б.*) человека (ст. 7 УК РФ). Таким образом, категория «безопасность» не только имеет нормативное употребление, но возведена в ранг принципиальных положений Уголовного закона, что определяет ее широкое юридическое значение, в том числе для целей классификации преступлений. В связи с этим отметим, что в Особенной части УК РФ термин «безопасность» употребляется 72 раза, включая 4 раза для терминологического определения отдельных родов и видов преступления (преступления против общественной безопасности, преступления против безопасности движения, преступления против безопасности государства, преступления против безопасности человечества).

Во-вторых, понятие кибернетики не столь эклектично по отношению к правовым категориям, как может показаться при первом приближении. Так, сформулированное в 1948 г. американским математиком Н. Винером определение, на наш взгляд, дает возможность весьма полно определить перечень определенных критериев, на основании которых можно говорить о деяниях в киберпространстве и сфере кибербезопасности.

Согласно определению Н. Винера, кибернетика – это наука об общих закономерностях *процессов управления и передачи информации* (курсив мой. – *Р. Б.*) в машинах, живых организмах и обществе. Заметим, что понимание вышеуказанных процессов может в уголовно-правовом дискурсе осуществляться с позиций объекта и предмета преступления, общественно опасных деяния и последствий, способа, орудий, средств и обстановки совершения преступления, а также в определенной интерпретации служить цели формулирования признаков специального субъекта рассматриваемых преступлений. Такая универсальность позволяет охватить весьма широкие границы понятия «киберпреступление», на что справедливо указывают многие специалисты [5, с. 59–60].

Теперь о видах преступлений в сфере кибербезопасности.

Анализ действующего уголовного законодательства РФ показывает, что с учетом сказанного выше взгляд на преступление в сфере кибербезопасности может быть очень широким. Так, к числу рассматриваемых преступлений, кроме тех, которые непосредственно связаны с компьютерной техникой, компьютерной информацией, информационно-телекоммуникационными сетями (в том числе Интернетом), электронными средствами передачи информации и платежа, средствами хранения, обработки или передачи компьютерной информации и т. д., могут быть отнесены многочисленные преступные деяния, в описании состава которых не содержится упоминания вышеперечисленных признаков.

Например, ч. 1 ст. 138 УК РФ предусматривает ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан. При этом в судебной практике под иными сообщениями понимаются сообщения граждан, передаваемые по сетям электрической связи, например СМС- и ММС-сообщения, факсимильные сообщения, передаваемые посредством сети «Интернет» мгновенные сообщения, электронные письма, видеозвонки и пр.

В ст. 276 УК РФ установлена ответственность за шпионаж в форме передачи, собирания, похищения или хранения в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну. Очевидно, что собирание и похищение указанных сведений может осуществляться с использованием компьютерной техники и т. п.

Еще один пример. В соответствии со ст. 290 УК РФ, предметом взятки может выступать незаконное предоставление имущественных прав, под которыми понимаются в том числе доходы от использования *цифровых пра*в (курсив мой. – *Р. Б.*). Кроме этого, Пленум Верховного

суда РФ в Постановлении от 09.07.2013 № 24 «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» отдельно разъясняет вопросы применения уголовного закона РФ, когда предмет взятки передается в виде зачисления денежных средств на «электронный кошелек».

Можно привести много других подобных примеров, которые служат свидетельством, что «киберпреступление» в самом широком понимании имеет место и в случаях, когда законодательное описание состава преступления не содержит прямого указания на «кибер»-признаки, в том числе «кибер»-характер.

С другой стороны, столь широкий подход вряд ли может оказаться продуктивным, если речь идет о решении задачи формулирования киберпреступлений как отдельного вида преступлений. В данном случае полезно выделить в тексте УК РФ и перечислить те признаки преступлений, которые позволяют относить данные преступления к категории «кибер».

Анализ показывает, что соответствующими признаками выступают несколько групп признаков (далее приводятся формулировки в точном соответствии с УК РФ).

Первая группа признаков связана с характеристикой объекта и предмета преступного посягательства, а именно:

1) совершение преступления **«в сфере компьютерной информации»** (гл. 28, ст. 272–274.2 УК РФ);

2) совершение преступления в отношении **«электронных средств, электронных носителей информации, технических устройств, компьютерных программ, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств»** (гл. 22, ст. 187 УК РФ).

Вторая группа признаков в различных аспектах характеризует обстановку, орудия, средства либо способ совершения преступления. В числе таковых:

1) совершение преступления **«в информационно-телекоммуникационных сетях (включая сеть «Интернет»)»**:

– доведение до самоубийства (гл. 16, ст. 110 УК РФ);

– склонение к совершению самоубийства или содействие совершению самоубийства (гл. 16, ст. 110.1 УК РФ);

– клевета (гл. 17, ст. 129.1 УК РФ);

– нарушение неприкосновенности частной жизни (гл. 19, ст. 137 УК РФ);

2) совершение преступления **«путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей»**: мошенничество в сфере компьютерной информации (гл. 21, ст. 159.6 УК РФ);

3) совершение преступления **«с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)»**:

– жестокое обращение с животными (гл. 25, ст. 245 УК РФ);

– незаконные добыча и оборот особо ценных диких животных и водных биологических ресурсов, принадлежащих к видам, занесенным в Красную книгу Российской Федерации и (или) охраняемым международными договорами Российской Федерации (гл. 26, ст. 258.1 УК РФ);

4) совершение преступления **«с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)»**:

– организация деятельности, направленной на побуждение к совершению самоубийства (гл. 16, ст. 110.2 УК РФ);

– понуждение к действиям сексуального характера (гл. 18, ст. 133 УК РФ);

– вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (гл. 20, ст. 151.2 УК РФ);

– незаконные организация и проведение азартных игр (гл. 22, ст. 171.2 УК РФ);

– манипулирование рынком (гл. 22, ст. 185.3 УК РФ);

– публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (гл. 24, ст. 205.2 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия, основных частей огнестрельного оружия, боеприпасов (гл. 24, ст. 222 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств (гл. 24, ст. 222.1 УК РФ);

– незаконные приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему (гл. 24, ст. 222.2 УК РФ);

– незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (гл. 25, ст. 228.1 УК РФ);

– склонение к потреблению наркотических средств, психотропных веществ или их аналогов (гл. 25, ст. 230 УК РФ);

– обращение фальсифицированных, недоброкачественных и незарегистрированных лекарственных средств, медицинских изделий и оборот фальсифицированных биологически активных добавок (гл. 25, ст. 238.1 УК РФ);

– незаконные изготовление и оборот порнографических материалов или предметов (гл. 25, ст. 242 УК РФ);

– изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (гл. 25, ст. 242.1 УК РФ);

– использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (гл. 25, ст. 242.2 УК РФ);

– публичные призывы к осуществлению экстремистской деятельности (гл. 29, ст. 280 УК РФ);

– публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (гл. 29, ст. 280.1 УК РФ);

– публичные призывы к осуществлению деятельности, направленной против безопасности государства (гл. 29, ст. 280.4 УК РФ);

– возбуждение ненависти либо вражды, а равно унижение человеческого достоинства (гл. 29, ст. 282 УК РФ);

– реабилитация нацизма (гл. 34, ст. 354.1 УК РФ).

Отметим, что в подавляющем большинстве случаев признаки «киберпреступления» указываются законодателем в рамках квалифицированных составов соответствующих преступлений.

Таким образом, можно выделить несколько возможных подходов к определению уголовно-правового содержания термина «преступление в сфере кибербезопасности».

Первый – максимально широкий: это преступление, объективные элементы состава которого не содержат вышеперечисленных признаков (например, «с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»)», но фактические обстоятельства совершения преступления свидетельствуют о наличии таковых.

При таком понимании, едва ли не каждое преступное деяние, предусмотренное УК РФ, может при определенных обстоятельствах обладать признаками «киберпреступления».

Второй – максимально узкий: это преступление, предусмотренное главой 28 УК РФ, объектом посягательства которого выступают общественные отношения в сфере кибербезопасности.

Выше можно было убедиться, что такой подход является усеченным.

Третий – сбалансированный: это преступление, состав которого содержит прямое указание на вышеперечисленные объективные признаки (например, объектом преступления выступают отношения в сфере критической информационной инфраструктуры РФ; предметом – компьютерная программа; способ совершения преступление – использование сети «Интернет» и т. д.).

Список литературы

1. Состояние преступности в России за январь-декабрь 2022 года / Отчет Главного информационно-аналитический центра МВД России [Электронный ресурс]. URL: https://мвд.рф/reports/item/35396677 (дата обращения: 12.05.2023).
2. **Данилов Р. М., Рыбак А. В.** Некоторые вопросы, связанные с преступлениями в сфере кибербезопасности // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2022. № 8. С. 45–51.
3. **Никульченкова Е. В.** О необходимости введения дефиниции «киберпреступление» в Уголовный закон Российской Федерации // Вестник Омского ун-та. Серия: Право. 2022. Т. 19, № 3. С. 98–107.
4. **Номоконов В. А., Тропина Т. Л.** Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1 (24). С. 45–55.
5. **Джафарли В. Ф.** Терминологические основы уголовно-правового обеспечения криминологической кибербезопасности (часть 2) // Ученые труды Российской академии адвокатуры и нотариата. 2022. № 2 (65). С. 56–61.

References

1. **The state of crime** in Russia for January-December 2022 / Report of the Main Information and Analytical Center of the Ministry of Internal Affairs of Russia [Electronic resource]. URL: https://mvd.rf/reports/item/35396677 (date of access: 05.12.2023).
2. **Danilov R. M., Rybak A. V.** Some issues related to cybersecurity crimes // Crime in the field of information and telecommunication technologies: problems of prevention, detection and investigation of crimes. 2022. No. 8. Pp. 45–51.
3. **Nikulchenkova E. V.** On the need to introduce the definition of “cybercrime” in the Criminal Law of the Russian Federation // Bulletin of the Omsk University. Series “Law”. 2022. Vol. 19, no. 3. Pp. 98–107.
4. **Nomokonov V. A., Tropina T. L.** Cybercrime as a new criminal threat // Criminology yesterday, today, tomorrow. 2012. No. 1 (24). Pp. 45–55.
5. **Jafarli V. F.** Terminological bases of criminal law support of criminological cybersecurity (part 2) // Scientific works of the Russian Academy of Advocacy and Notaries. 2022. No. 2 (65). Pp. 56–61.

Информация об авторе

Роман Николаевич Боровских, доктор юридических наук

Information about the Author

Roman N. Borovskikh, Doctor of Law

Статья поступила в редакцию 15.05.2023;
одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 15.05.2023;
approved after reviewing 21.06.2023; accepted for publication 31.07.2023

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

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 автоматизации [1]. 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 расходов[3].

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, ссылался 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

Научная статья

УДК 346.57
DOI 10.25205/2542-0410-2023-19-3-30-37

Правовые проблемы построения внутрикорпоративной системы комплаенса в области защиты персональных данных

Елена Анатольевна Дорожинская

Сибирский институт управления – филиал Российской академии народного хозяйства
и государственной службы при Президенте РФ
Новосибирск, Россия

sofia_1974@mail.ru

Аннотация

В статье анализируются нормы законодательства, позволяющие определить требуемые элементы внутрикорпоративной системы комплаенса в области защиты персональных данных в современных правовых условиях. Исследуется корпоративная и судебная практика, отражающая изменение правового регулирования комплаенса организаций в сфере сбора и использования персональных данных, формируются рекомендации по разработке внутренних документов корпорации, регламентирующих обработку персональных данных корпорации.

Ключевые слова

персональные данные, комплаенс, участники общества, корпоративное управление, внутренние документы

Для цитирования

Дорожинская Е. А. Правовые проблемы построения внутрикорпоративной системы комплаенса в области защиты персональных данных // Юридическая наука и практика. 2023. Т. 19, № 3. С. 30–37. DOI 10.25205/2542-0410-2023-19-3-30-37

Legal Problems of Building an Internal Corporate Compliance System in the Field of Personal Data Protection

Elena A. Dorozhinskaya

Siberian Institute of Management – a branch of the Russian Academy of National Economy
and Public Administration under the President of the Russian Federation
Novosibirsk, Russia

sofia_1974@mail.ru

Abstract

The article analyzes the norms of legislation that allow to determine the required elements of the internal corporate compliance system in the field of personal data protection in modern legal conditions. The corporate and judicial practice, reflecting the change in the legal regulation of the compliance of organizations in the field of collection and use of personal data, is being studied, recommendations are being formed for the development of internal documents of the corporation that regulate the processing of personal data of the corporation

Keywords

personal data, compliance, company members, corporate governance, internal documents

For citation

Dorozhinskaya E. A. Legal problems of building an internal corporate compliance system in the field of personal data protection. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 30–37. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-30-37

Прежде чем анализировать причины проблем, возникающих при построении внутрикорпоративной системы комплаенса в области защиты персональных данных, надо определить особенности этой системы, цель ее внедрения в деятельность корпораций и ожидаемый результат.

Понятие «комплаенса» внедряется в российское законодательство и практику весьма осторожно и поэтапно, при этом его направления радикально разнообразны. Кроме того, само понятие комплаенса используется в различных смыслах, исходя из сферы его применения.

К примеру, первоначально определение комплаенс-контроля было дано в указании Банка России от 7 июля 1999 г. № 603-У «О порядке осуществления внутреннего контроля за соответствием деятельности на финансовых рынках законодательству о финансовых рынках в кредитных организациях» и некоторое время использовалось исключительно в финансово-экономической сфере.

Позже с принятием Федерального закона от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции», дополненным в 2012 г. статьей 13.3 об обязанностях организаций разрабатывать и принимать меры по предупреждению коррупции, в употребление вошло понятие «антикоррупционного комплаенса». В дальнейшем его определение было сформулировано в п. 2 «Методических рекомендаций по разработке и принятию организациями мер по предупреждению и противодействию коррупции» [1] на основе эклектичного сочетания подходов к комплаенсу как процессу (обеспечение соответствия деятельности организации установленным требованиям) и как системе мер, обеспечивающих комплексную защиту организации.

В дальнейшем внедрение систем комплаенса стало все более популярным в предпринимательской среде, поскольку оказалось, что превентивно разработать и внедрить в корпорации механизмы обеспечения соблюдения законодательства в различных направлениях гораздо выгодней, чем нести ответственность за нарушения законодательства постфактум.

Безусловно, формирование системы комплаенса в конкретной организации требует особого подхода в зависимости от масштаба корпорации, ее организационно-правовой формы и системы корпоративного управления, сферы деятельности и т. д. Кроме того, для крупных корпораций неизбежно формирование либо нескольких систем, либо сложной многоуровневой системы комплаенса в зависимости от императивных установок законодательства и направлений необходимого контроля.

Например, кроме упомянутых выше направлений банковского и антикоррупционного комплаенса, часто применяются антимонопольный налоговый, трудовой, и даже так называемый «санкционный» комплаенс. Применительно к исследуемой теме далее будет использоваться термин «информационный комплаенс», хотя, безусловно, его смысл, исходя из содержания понятия «информация» гораздо шире, чем того требует обеспечение контроля за соблюдением законодательства об обработке именно персональных данных.

Общеизвестно, что в действующей редакции ст. 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон №152-ФЗ) понятие персональных данных трактуется максимально широко – как «любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)»,

[1] Методические рекомендации по разработке и принятию организациями мер по предупреждению и противодействию коррупции (с изм. на 8 апреля 2014 г.). URL: https://docs.cntd.ru/document/499057913 (дата обращения: 12.04.2023).

что усложняет формирование универсального подхода к построению внутрикорпоративной системы информационного комплаенса.

Ведь, кроме общепринятых данных о лице типа «фамилия, имя, отчество, дата и год рождения, место жительства» и прочее, к персональным данным может относиться в принципе любая информация о субъекте. Например, персональными данными признаются «абонентский номер или адрес электронной почты… в случае, когда такая информация относится к прямо или косвенно определенному или определяемому физическому лицу»[2], «хэш-ID пользователя – уникальный идентификатор активного пользователя сети сотовой связи»[3], все государственные идентификаторы физического лица (ИНН, СНИЛС) и т. д. Поэтому формирование системы информационного комплаенса внутри корпорации может изначально потребовать масштабного анализа реальных потребностей организации исходя из направлений ее деятельности и субъектного состава.

Статья 18.1 Закона №152-ФЗ с 2011 г. установила базовые требования к построению информационного комплаенса в организациях – «операторах персональных данных», определив Роскомнадзор в качестве контролирующего органа (уполномоченного органа по защите прав персональных данных). В числе обязательных мер Закон называет назначение в организации лица, ответственного за организацию обработки персональных данных, разработку и издание пакета документов, определяющих политику корпорации в отношении обработки этих данных, организацию мер по обеспечению их безопасности, осуществлению внутреннего контроля и (или) аудита, а также ознакомлению работников корпорации с действующим законодательством и установленными требованиями в этой области. В целом перечисленные меры по формированию внутриорганизационной системы комплаенса традиционны, но с учетом использования персональных данных для достижения уставных целей корпораций возникают характерные особенности как для различных организационно-правовых форм организаций, так и для различных сфер их деятельности.

Прежде чем перейти к особенностям регулирования обработки персональных данных участников корпоративных отношений, стоит вспомнить нормы гражданского законодательства о том, что корпоративные отношения внутри организации могут регулироваться внутренними регламентами и иными внутренними документами юридического лица (п. 5 ст. 52 Гражданского кодекса РФ). При этом возникает вопрос о соотношении и разграничении «внутреннего регулирования» и «локального регулирования» отношений внутри организации, применительно к которым действуют нормы трудового законодательства. По мнению автора, при построении системы информационного комплаенса в организации эти сферы нуждаются в разграничении по причине различия целей контроля.

Законом установлены требования к предоставлению и раскрытию информации корпорацией, что однозначно повлечет необходимость предоставления доступа к персональным данным определенному или неопределенному кругу лиц. При этом начать построение системы информационного комплаенса стоит с определения перечня документов, в которых содержатся либо могут содержаться подобные сведения. В этот перечень могут входить журнал регистрации акционеров (участников) на общем собрании; список лиц, имеющих право участвовать в общем собрании участников; запросы акционеров в общество; доверенности для оформления участия в общем собрании акционеров; бухгалтерские документы, протоколы общих собраний и собраний совета директоров; списки аффилированных лиц; сообщения о существенных фактах и т. д. Отдельного внимания заслуживает перечень документов, оформляющих трудовые

[2] О разъяснении норм федерального законодательства: письмо Минкомсвязи России от 7 июля 2017 г. № П11-15054-ОГ. URL: https://www.consultant.ru/document/cons_doc_LAW_220762/ (дата обращения: 12.04.2023).

[3] Постановление Тринадцатого апелляционного арбитражного суда от 1 июля 2016 г. по делу № А56-6698/2016. URL: https://sudact.ru/arbitral/doc/J8ihyq5cYyo1/ (дата обращения: 12.04.2023).

отношения с единоличным исполнительным органом: трудовой договор и трудовая книжка, документы, подтверждающие получение образования, копия паспорта, копии документов о заключении брака, рождении детей и т. д.

С другой стороны, Закон №152-ФЗ устанавливает условия обработки персональных данных в различных случаях, формируя как ограничения, так и возможности для построения информационного комплаенса в организации.

Например, в конце 2020 г. в Законе №152-ФЗ появилась новая статья 10.1, регулирующая обработку персональных данных, разрешенных субъектом для распространения в неопределенном кругу лиц. Если до этого момента организации было достаточно разработать «Политику конфиденциальности персональных данных», выставить ее на сайт и предоставить субъекту техническую возможность с ней согласиться (путем «нажатия кнопки»), то сейчас право на распространение таких данных должно быть оформлено отдельным согласием. Форма согласия была утверждена позднее приказом Роскомнадзора от 24 февраля 2021 г. № 18 [4], а сама обязанность обеспечена обновлением мер ответственности в ст. 13.1 КоАП РФ.

Для корпорации может стать проблемой тот факт, что лицо может отозвать свое согласие и потребовать прекратить распространение своих персональных данных, несмотря на ранее соблюденные требования и правомерность их использования. Законодатель точечно установил запрет на отзыв согласия, но он касается только тех ситуаций, когда обработка персональных данных осуществляется в целях выполнения публичных функций и полномочий государственными и муниципальными органами, которыми корпорации не являются (п. 15 ст. 10.1 Закона № 152-ФЗ). Для самой корпорации негативный эффект может проявиться в зависимости от статуса и значимости данных о субъекте, отозвавшем свое согласие.

В этой связи стоит отметить, что внутренняя регламентация построения в корпорации системы информационного комплаенса делится на два базовых направления регулирования обработки персональных данных. Первое направление связано с обработкой персональных данных участников корпоративных отношений, второе направление – иных субъектов, участвующих и обеспечивающих деятельность корпорации как организации в целом (например, работников).

Что касается разновидностей корпоративных отношений, связанных с обработкой персональных данных, то особое внимание стоит обратить на деятельность хозяйственных обществ. Больше всего норм, связанных с персональными данными, содержится в федеральных законах от 26 декабря 1995 г. №208-ФЗ «Об акционерных обществах» (далее – Закон №208-ФЗ) и от 8 февраля 1998 г. № 14-ФЗ «Об обществах с ограниченной ответственностью» (далее – Закон №14-ФЗ), что неудивительно, поскольку именно эти организационно-правовые формы корпораций являются наиболее распространенными.

Вообще корпоративная деятельность неразрывно связана со сбором и обработкой информации. В корпоративных отношениях есть масса позиций для физического лица, в которых оно непосредственно становится субъектом персональных данных. Это, в частности, проявляется, когда гражданин является:

– акционером либо участником общества с ограниченной ответственностью;

– единоличным исполнительным органом или членом коллегиального исполнительного органа корпорации;

– членом совета директоров корпорации.

К персональным данным первой группы субъектов можно отнести не только фамилию, имя и отчество лица, но и его фактический корпоративный статус (участник, акционер и т. д.),

[4] Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 24 февраля 2021 г. № 18. URL: https://base.garant.ru/400668442/ (дата обращения 12.04.2023).

количество принадлежащих ему акций либо размер доли в уставном капитале общества, основания приобретения акций либо долей и т. д. К данным субъектов второй группы, участвующих в управлении обществом, кроме прочего, относится фактическая должность и основания ее замещения, размер вознаграждения, факт и основания прекращения полномочий (если таковое случилось) и т. д. Как видно, перечень сведений, составляющий объем персональных данных для этих лиц, не является закрытым и зависит от наличия и объема их корпоративных прав.

Кроме вышесказанного, корпорация как юридическое лицо не только фактически обладает информацией о своих участниках и членах органов управления, но также хранит ее и совершает с ней установленные законом действия, что подтверждает статус корпорации как оператора персональных данных. В частности, документы общества, предоставляемые по запросу участника в соответствии с требованиями закона, могут содержать персональные данные либо раскрывать информацию о крупных и аффилированных участниках, членах совета директоров, юридических лицах, в которых работают заинтересованные лица и члены их семей. При этом к персональным данным в том числе может применяться режим конфиденциальной информации (если их владелец не давал разрешения на публичное представление в средствах массовой информации).

Но стоит разделять факт отнесения информации к персональным данным и обязанность по сохранению конфиденциальности персональных данных. В корпоративных отношениях эти явления связаны не всегда, поскольку возникает вопрос соотношения частных и публичных интересов. Под частным интересом в данном контексте понимается интерес гражданина, заключающийся в сохранении его персональных данных, а под публичным понимается интерес всех остальных субъектов (включая государство) в получении информации о том, что гражданин состоит в корпоративных отношениях. Можно предположить, что баланс смещен в сторону поддержки публичного интереса. Это подтверждается давними и известными позициями Конституционного суда РФ, отраженными в Постановлении от 24 февраля 2004 г. №3-П[5], определении от 18 января 2011 г. №8-О-П [6] и т. д.

Кроме того, это подтверждается анализом содержания ст. 7 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон № 149-ФЗ) в совокупности со ст. 6 Закона № 152-ФЗ, устанавливающих освобождение от обязанности сохранять конфиденциальность общедоступных (однажды разглашенных) персональных данных. Применительно к деятельности корпораций эти нормы получают интересную трактовку.

Например, возникает вопрос относительно сохранения режима персональных данных в отношении вносимых в Единый государственный реестр юридических лиц на основании Федерального закона от 8 августа 2001 г. № 129-ФЗ «О государственной регистрации юридических лиц и индивидуальных предпринимателей» сведений о гражданине – единоличном исполнительном органе или об участнике корпорации (фамилия, имя, отчество, должность). Поскольку имеет место свободный доступ любого лица к выписке из Единого государственного реестра юридических лиц, в которой фигурируют в том числе и индивидуальные номера налогоплательщиков, позволяющие однозначно идентифицировать названных лиц, то можно

[5] По делу о проверке конституционности отдельных положений статей 74 и 77 Федерального закона «Об акционерных обществах», регулирующих порядок консолидации размещенных акций акционерного общества и выкупа дробных акций, в связи с жалобами граждан, компании «Кадет Истеблишмент» и запросом Октябрьского районного суда города Пензы: постановление Конституционного суда РФ от 24.02.2004 № 3-П. URL: http://www.consultant.ru/document/cons_doc_LAW_46768/#dst100025 (дата обращения: 12.04.2023).

[6] По жалобе открытого акционерного общества «Нефтяная компания «Роснефть»» на нарушение конституционных прав и свобод положением абзаца первого пункта 1 статьи 91 Федерального закона «Об акционерных обществах»: определение Конституционного суда РФ от 18.01.2011 № 8-О-П. URL: http://www.consultant.ru/document/cons_doc_LAW_110660/ (дата обращения: 12.04.2023).

сделать вывод, что эти данные являются общедоступной информацией, поскольку указанные граждане были осведомлены о возможных последствиях их участия в корпорации.

С другой стороны, общедоступными являются, как правило, не все данные относительно корпоративных субъектов, например, нельзя получить сведения о доходах лица из объективно открытых источников. Но и в этом случае имеются исключения, что было отражено еще в Информационном письме Президиума ВАС РФ от 18 января 2011 г. № 144 [7], где суд уточнил, что «не требуется согласия физических лиц, вступивших в правоотношения с обществом, на предоставление участнику хозяйственного общества документов, содержащих персональные данные таких физических лиц». Это отразилось на судебной практике, например, в постановлении Президиума ВАС РФ от 22 мая 2012 г. № 16803/11 суд квалифицировал требование акционеров о предоставлении копии трудового договора с руководителем организации как правомерное. Несмотря на то что договор содержал сведения о заработной плате директора, относящиеся к персональным данным, суд счел, что акционеры вправе получить эту информацию, так как размер выплат руководителю влияет на стоимость акций, а значит, связан с обеспечением интересов акционеров [1].

Отдельно стоит рассмотреть вопрос об отождествлении как статуса, так и репутации организации и ее руководителя, находящем отражение в регламентации использования персональных данных. Как известно, персональные данные могут относиться только к физическому лицу (ст. 3 закона №152-ФЗ), а в процессе учреждения организации регистрационный орган получает доступ и к персональным данным его руководителя, участников и т. д. Но для идентификации юридического лица в целом потребность в использовании персональных данных его участников отсутствует. Поэтому когда, в частности, возникает вопрос о защите деловой репутации корпорации и ее руководителя в результате публикации недостоверных сведений в сети «Интернет», законодательство и судебная практика разграничивает эти механизмы, так как Закон № 152-ФЗ регулирует обращение персональных данных гражданина, а Закон № 149-ФЗ – в том числе и юридических лиц [8].

Ведя речь о формировании мер информационного комплаенса в отношении работников корпорации, стоит отметить спорные вопросы, некоторые из которых со временем разрешились, а некоторые актуальны по сей день.

Например, при предоставлении работодателем своим работникам корпоративных симкарт ранее возникала коллизия, связанная с необходимостью получения их согласия на передачу персональных данных работника оператору связи. Проблема была устранена введением в 2017 г. в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» снимающего такую потребность абзаца 7 п. 1 ст. 53.

С другой стороны, в результате цифровизации деятельности корпораций все большее внимание стало уделяться содержанию их сайтов, представляющих организацию в сети «Интернет», а также позволяющих решать рабочие задачи. Таким образом, возникла проблема надлежащего урегулирования обработки биометрических персональных данных сотрудников, влекущей необходимость получения отдельного согласия [2, с. 43]. И в некоторых случаях она действительно актуальна, несмотря на ряд исключений, закрепленных в действующем законодательстве, например, в ст. 152.1 Гражданского кодекса РФ, устанавливающей случаи, когда такого согласия не требуется (например, когда изображение гражданина получено при съемке, проведенной на публичных мероприятиях). В остальных случаях у работодателя возникает

---

[7] О некоторых вопросах практики рассмотрения арбитражными судами споров о предоставлении информации участникам хозяйственных обществ: информационное письмо Президиума ВАС РФ от 18.01.2011. № 144. URL: http://www.consultant.ru/document/cons_doc_LAW_110485/ (дата обращения: 12.04.2023).

[8] Решение арбитражного суда Краснодарского края от 3 декабря 2019 года по делу № А32-42912/2019. URL: https://sudact.ru/arbitral/doc/kxbQEZ7sNCLc/ (дата обращения: 12.04.2023).

необходимость регламентировать локальными актами порядок разработки и наполнения сайта организации, ознакомить с ним сотрудников в порядке ст. 74 Трудового кодекса РФ, а также получить от них необходимые согласия.

Можно также сделать вывод о необходимости превентивного регулирования на уровне системы информационного комплаенса действий операторов, которые в последние годы порождают активное привлечение их к ответственности по ч. 2 ст. 13.11 КоАП РФ. По данным Роскомнадзора за 2022 г., чаще всего наблюдается:

– неправомерная обработка биометрических персональных данных работника в целях прохода на территорию оператора-работодателя и учета рабочего времени (нарушение ч.1 ст. 11 и ч. 4 ст. 9 Закона № 152-ФЗ);

– неправомерное осуществление трансграничной передачи персональных данных на территорию стран, не обеспечивающих адекватную защиту (командирование работников, технологическое сопровождение кадровой информационной системы персональных данных, дающей доступ к данным работника) (ч. 4 ст. 12 и ч. 4 ст. 9 Закона № 152-ФЗ);

– неправомерная передача персональных данных работников в адрес третьих лиц (в рамках добровольного медицинского страхования, изготовления визитных карточек, реализации зарплатного проекта, аутсорсинга и т. д.) (нарушение требований ст. 88 ТК РФ и ч. 4 ст. 9 Закона № 152-ФЗ) [3][9].

Еще один аспект должен найти отражение при построении системы информационного комплаенса внутри корпорации. Речь идет о регламентации обработки персональных данных граждан, доступ к которым корпорация получает в ходе осуществления своей целевой уставной деятельности. Это может быть, например, гражданин – клиент банка, оформляющий кредитный договор, данные которого банк передает страховой организации, потребитель, осуществляющий онлайн-платежи, когда данные плательщика получает оператор – интернет-магазин, либо лицо, получающее услугу опосредованно от основного контрагента (оператора), передавшего ее на аутсорсинг. Также имеют место случаи неправомерной обработки и передачи оператором персональных данных третьим лицам, осуществляющим телефонные звонки в целях взыскания просроченной задолженности при отсутствии правовых оснований на такие действия.

Стоит обратить особое внимание на особенности обработки, хранения и анализа корпорациями в ходе своей работы с клиентами и контрагентами так называемых «больших данных» (*big data*), или «больших массивов данных», позволяющих более успешно достигать предпринимательских целей. В рамках рассматриваемой темы можно констатировать, что использование больших массивов данных становится эффективным тогда, когда обрабатываются пользовательские персональные данные граждан, использующих сеть «Интернет». В данных случаях без надлежащего оформления обработки персональных данных деятельность корпорации невозможна. Надлежащее обеспечение их сохранности возлагается на саму организацию, которая должна использовать все доступные средства (включая информационно-технические) для защиты информации о клиентах.

В результате проведенного анализа теории и практики регулирования и обработки персональных данных можно сделать некоторые выводы относительно основных условий формирования внутрикорпоративной системы информационного комплаенса.

1. Перед разработкой документации, обеспечивающей систему информационного комплаенса, необходимо определить перечень законных оснований для обработки персональных данных в конкретной организации в рамках целей ее деятельности.

2. Система комплаенса должна обеспечивать соблюдение общих принципов обработки персональных данных, особенно принципа минимизации данных, исключающей их избыточ-

[9] Онлайн-семинар Роскомнадзора, приуроченный к Международному дню защиты персональных данных. 28 января 2022 г. URL: https://rkn.gov.ru/news/rsoc/news74044.htm (дата обращения: 12.04.2023).

ность; принципа целевой обработки данных, а также принципа оптимизации данных путем их удаления либо обезличивания по достижении цели обработки и устранения потребности в них.

3. Система комплаенса должна формироваться с учетом императивных требований законодательства относительно обязательного уведомления уполномоченного органа о намерениях обработки данных, а также о случившихся утечках, локализации баз данных на территории Российской Федерации, соблюдения порядка трансграничной передачи данных и т. д.

Соблюдение этих условий, по мнению автора, позволит в пределах конкретной корпорации сформировать оптимальный и действенный механизм обеспечения соответствия деятельности организации требованиям действующего законодательства о персональных данных.

Список литературы

1. **Титов Д. М.** Персональные данные в корпоративных правоотношениях // Акционерное общество. 2016. № 3 (142). URL: https://ao-journal.ru/personalnye-dannye-v-korporativnyk-pravootnosenijk (дата обращения: 12.04.2023).
2. **Королева Я. Ю.** Изменения в законодательстве, касающиеся персональных данных // Руководитель бюджетной организации. 2022. № 8. С. 42–49.
3. **Куревина Л.** Ответственность за нарушение требований в области персональных данных // Казенные учреждения: бухгалтерский учет и налогообложение. 2021. № 5. URL: https://base.garant.ru/77247525/ (дата обращения: 12.04.2023).

References

1. **Titov D. M.** Personal data in corporate legal relations. *Joint-Stock Company*. 2016. № 3 (142). URL: https://ao-journal.ru/personalnye-dannye-v-korporativnyk-pravootnosenijk (date of access: 12.04.2023) (in Russ.)
2. **Koroleva Y. Y.** Changes in legislation concerning personal data. *Head of a budgetary organization*. 2022. № 8. P. 42–49.
3. **Kurevina L.** Responsibility for violation of requirements in the field of personal data. *Treasury institutions: accounting and taxation*. 2021. № 5. URL: https://base.garant.ru/77247525/ (дата обращения: 12.04.2023) (in Russ.)

Информация об авторе

Елена Анатольевна Дорожинская, кандидат юридических наук

Information about the Author

Elena A. Dorozhinskaya, PhD in Law

Статья поступила в редакцию 13.04.2023;
одобрена после рецензирования 10.05.2023; принята к публикации 31.07.2023

The article was submitted 13.04.2023;
approved after reviewing 10.05.2023; accepted for publication 31.07.2023

Научная статья

УДК 346
DOI 10.25205/2542-0410-2023-19-3-38-46

Конфиденциальность персональных данных в ситуации киберугроз

Елизавета Владимировна Зайнутдинова

Новосибирский национальный исследовательский государственный университет
Новосибирск, Россия

zainutdinovaev@gmail.com

Аннотация

Несмотря на наличие действующего правового регулирования персональных данных и их оборота в сети «Интернет», за последнее время Россия стала одним из лидеров по утечкам персональных данных. Получается, что право на конфиденциальность и право на защиту персональных данных не реализуются в цифровой среде ввиду подверженности кибератакам и отсутствия надлежащих мер и гарантий в указанной сфере. Российский законодатель устанавливает обязательства оператора персональных данных, в том числе обязанность оператора уведомить уполномоченный орган об утечке персональных данных, а также административную, уголовную и гражданско-правовую ответственность за их разглашение. Однако действенные механизмы, которые бы препятствовали превентивно утечкам и иному разглашению персональных данных, позволяли бы в полной мере компенсировать причиненный физическим лицам ущерб, отсутствуют. В правовой доктрине предлагается усилить меры ответственности за нарушения в сфере персональных данных и конкретизировать возможность возмещения морального вреда пострадавшим от утечки лицом. Авторский подход заключается в закреплении необходимости проведения проверки деятельности оператора на предмет нарушений, приведших к утечке персональных данных (пост-контроль), во внедрении комплаенс-системы, позволяющей превентивно предотвращать утечки и иные нарушения в сфере персональных данных (априори-контроль), а также обучении сотрудников для минимизации рисков разглашения и иного незаконного использования персональных данных.

Ключевые слова

персональные данные, киберугрозы, конфиденциальность, цифровая среда, утечки, сеть «Интернет», идентификация, защита персональных данных

Для цитирования

Зайнутдинова Е. В. Конфиденциальность персональных данных в ситуации киберугроз // Юридическая наука и практика. 2023. Т. 19, № 3. С. 38–46. DOI 10.25205/2542-0410-2023-19-3-38-46

Confidentiality of Personal Data in Case of Cyberthreats

Elizaveta V. Zainutdinova

Novosibirsk National Research State University
Novosibirsk, Russian Federation

zainutdinovaev@gmail.com

Abstract

Despite the presence of the current legal regulation of personal data and their circulation on the Internet, Russia has recently become one of the leaders in personal data leaks. It turns out that the right to confidentiality and the right to protection of personal data are not implemented in the digital environment due to the susceptibility to cyberattacks and the

lack of appropriate measures and guarantees in this field. The Russian legislator establishes the obligations of the operator of personal data, including the obligation of the operator to notify the authorized body of the leakage of personal data, as well as administrative, criminal and civil liability for their disclosure. However, there are no effective mechanisms that would prevent leaks and other disclosure of personal data in a preventive manner and would allow full compensation for the damage caused to individuals. The legal doctrine proposes to strengthen the penalties for violations in the field of personal data and specify the possibility of compensation for moral damage to a person who has suffered from a leak. The author's approach is to provide for the need to check the operator's activities for violations that led to the leakage of personal data (post-control), as well as to introduce a compliance system that allows preventive prevention of leakages and other violations in the field of personal data (a priori control), and train employees to minimize the risks of disclosure and other illegal use of personal data.

Keywords

personal data, cyberthreats, confidentiality, digital environment, leaks, Internet, identification, protection of personal data

For citation

Zainutdinova E. V. Confidentiality of Personal Data in Case of Cyberthreats. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 38–46. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-38-46

Проблематика исследуемой темы

Персональные данные в настоящее время являются ценным ресурсом в сфере предпринимательского оборота и одновременно выступают объектом различного рода кибератак и утечек при совершении злонамеренных действий. Недавние прецеденты показывают, что конфиденциальность персональных данных находится под серьезной угрозой.

В соответствии с Федеральным законом «О персональных данных»[1], обеспечивается конфиденциальность персональных данных и гарантируется их защита, в том числе в цифровой среде. Так ли это на самом деле? Анализ последних дел показывает, что необходимы действенные механизмы защиты прав и воздействия на правонарушителей, которые бы позволили сделать защиту персональных данных реальной.

Так, совсем недавним случаем является утечка персональных данных сотрудников, студентов и абитуриентов Высшей школы экономики[2]. Несмотря на то что расследование утечки персональных данным образовательным учреждением было произведено в срок, в соответствии с частью 3.1 статьи 21 Федерального закона «О персональных данных»[3] Роскомнадзор был уведомлен об указанной ситуации, судебный участок мирового судьи № 387 по Басманному району г. Москвы оштрафовал Высшую школу экономики на 60 тысяч рублей за утечку персональных данных по части 1 статьи 13.11 КоАП РФ («Обработка персональных данных в случаях, не предусмотренных законодательством РФ»).

Более известной ситуацией является утечка данных пользователей «Яндекс.Еда», в результате которой в открытом доступе оказались персональные данные 58 тысяч пользователей.

---

[1] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // Российская газета. 2006. 29 июля. № 165.

[2] Безопасность данных сотрудников и студентов. Что делает Вышка для восстановления работы сервисов. Вышка для своих. 09 марта 2023 г. URL: https://www.hse.ru/our/news/819321304.html (дата обращения: 01.06.2023).

[3] См. подробнее: Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных» (зарегистрирован 28.12.2022 № 71851). URL: http://publication.pravo.gov.ru/Document/View/0001202212280052 (дата обращения: 02.06.2023).

Лишь не более двадцати из них получили небольшие компенсации[4]. ООО «Яндекс.Еда» было привлечено к административному штрафу в размере 60 тысяч рублей[5]. Таким образом, проблемы с конфиденциальностью персональных данных остались не решенными до сих пор.

Конфиденциальность не только персональных данных оказывается под угрозой: следует обратить внимание на взлом сайтов судов и иных государственных органов, например, Министерства по чрезвычайным обстоятельствам (ссылки на взлом сайтов судов и МЧС). Это все не может не вызывать беспокойства среди населения и не повышает общий уровень конфиденциальности особо охраняемой законодательством информации, в том числе персональных данных.

В России известна деятельность бирж, на которых происходит покупка и обмен персональными данными, а также даркнет-форумов[6], на которых можно оставить запрос о приобретении тех или иных персональных данных. Определенные риски для утечки персональных данных представляют собой и новые сервисы, такие как сервис облачного хранения пользовательских данных и ChatGPT – сервис искусственного интеллекта, на котором лица размещают свои персональные данные и который также не защищен от возможных кибератак и неправомерного получения и использования персональных данных. Все это затрагивает повседневную жизнь граждан и препятствует эффективному применению законодательства о персональных данных, реальности права на конфиденциальность и защиту персональных данных.

Следует отметить, что указанные проблемы не являются совсем уж новыми и характерными только для России. За рубежом также возникают проблемы с конфиденциальностью персональных данных. Из недавних дел можно отметить хакерский взлом принадлежащего компании Microsoft почтового клиента Outlook[7].

Таким образом, возникает вопрос о том, каким образом возможно обеспечить и улучшить конфиденциальность персональных данных в текущей ситуации: кибератак и киберугроз, в ситуации, когда персональные данные размещаются на серверах, расположенных в сети «Интернет», могут попасть в открытый доступ и использоваться злоумышленниками. Какие меры могут быть предприняты?

Для начала рассмотрим действующее правовое регулирование для того, чтобы оценить подход законодателя к текущей ситуации и возможные перспективы изменения законодательства.

Имеющиеся подходы законодателя и правоприменителя к утечкам персональных данных

Подход законодателя заключается в установлении правового режима персональных данных через их определение и ограничение возможностей оператора персональных данных по их использованию (ст. 3, 10, 11, 18, 18.1, 19 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ). Случаи неправомерного завладения персональными данными

---

[4] Информация по гражданским делам первой инстанции. Сторона: ООО «Яндекс.Еда». Официальный портал судов общей юрисдикции г. Москвы. Замоскворецкий районный суд URL: https://mosgorsud.ru/rs/zamoskvoreckij/services/cases (дата обращения: 02.06.2023).

[5] Информация по судебному делу № 05-0413/101/2022. Портал единого информационного пространства мировых судей г. Москвы. Судебный участок мирового судьи № 101. URL: https://mos-sud.ru/101/cases/admin/details/f6ffad43-95ae-4186-8d87-5e0ab277e669?respondent=ООО+%22ЯНДЕКС.ЕДА%22 (дата обращения: 02.06.2023).

[6] Что такое даркнет и почему там продаются наши данные. Индустрия 4.0. РБК Тренды URL: https://trends.rbc.ru/trends/industry/602f668a9a7947d5f06e0c7a (дата обращения: 02.06.2023)

[7] Microsoft fixes Outlook zero-day used by Russian hackers since April 2022. Bleeping Computer. March 14, 2023. URL: https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-outlook-zero-day-used-by-russian-hackers-since-april-2022/ (дата обращения: 02.06.2023).

составляют составы уголовного[8] и административного правонарушения[9]. Как правило, последствием нарушения законодательства о персональных данных выступает привлечение к административной ответственности по статье 13.11 Кодекса РФ об административных правонарушениях от 30.12.2001 № 195-ФЗ (далее – КоАП РФ). Статья 13.14 КоАП РФ применяется в тех случаях, когда лицо, получившее доступ к персональным данным в связи с исполнением служебных или профессиональных обязанностей, допустило их разглашение[10], что нередко можно встретить на практике и что выступает предпосылкой для утечек персональных данных.

Как показывает практика, уголовная ответственность наступает за более тяжкие деяния, которые заключаются не просто в разглашении персональных данных или в их ином незаконном использовании, а в причинении вреда имущественным или личным неимущественным правам субъекта. Как пример причинения такого вреда можно привести рассылку личных сообщений, фото или видео гражданина третьим лицам или размещение их во всеобщем доступе (см.: Кассационное определение Седьмого кассационного суда общей юрисдикции от 10.06.2020 № 77-889/2020) [1]. При этом такое разглашение зачастую имеет место путем размещения информации в Интернете[11].

В доктрине, в целом, отмечается, что утечка, составляющая состав административного правонарушения, может являться следствием как умышленных действий оператора персональных данных (его работников), так и выступать результатом хакерской атаки на информационные системы оператора в ситуациях, когда оператор не предпринял достаточных и разумных мер защиты [2].

Также подразумевается гражданско-правовая ответственность за утечки персональных данных, но дела крайне редки и суммы компенсаций незначительны, как было показано в судебной практике выше. Субъекты персональных данных вправе взыскивать наступившие убытки и возмещать причиненный моральный вред, но примеров достойных компенсаций за утечки персональных данных не встретишь. Соответственно, компании не так пекутся о принятии соответствующих мер, в том числе комплаенса, которые бы позволили предотвратить утечки персональных данных в будущем. То есть не до конца ясен ответ на вопрос, каким образом может получить лицо, пострадавшее от утечки, защиту от неправомерного использования и распространения своих персональных данных.

Недавно в законодательстве появилась уже упомянутая выше часть 3.1 статьи 21 Федерального закона «О персональных данных», регламентирующая порядок действий оператора при утечке персональных данных, его обязательство уведомить об этом Роскомнадзор, но нельзя заметить, что все обнаруженные на практике проблемы были решены. Уведомление о произошедших утечках, действительно, необходимо, но не позволяет превентивно их предотвращать.

Ввиду этого высказываются различные точки зрения и предлагаются законопроекты по совершенствованию действующего законодательства о персональных данных. Предлагается, ви-

---

[8] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.04.2023). Статья 137 // Собрание законодательства Российской Федерации. 17.06.1996. № 25. Ст. 2954.

[9] См.: Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 28.04.2023, с изм. от 17.05.2023). Статья 13.11 // Собрание законодательства РФ. 07.01.2002. № 1 (ч. 1). Ст. 1.

[10] Ответы на часто задаваемые вопросы к ст. 6 ФЗ от 27.07.2006. № 152-ФЗ «О персональных данных» «Условия обработки персональных данных». 2023 // СПС «КонсультантПлюс».

[11] Постановление Пленума Верховного суда Российской Федерации от 25.12.2018 № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (ст. 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» // СПС «КонсультантПлюс».

димо, по аналогии с европейским регламентом по защите данных GDPR[12], закрепить оборотные штрафы в отношении операторов, допустивших неправомерную или случайную передачу (предоставление, распространение, доступ) в отношении персональных данных, т. е., по сути, утечку персональных данных. Предлагается также установить уголовную ответственность за незаконный сбор, хранение, использование и передачу баз персональных данных, что направлено на борьбу с последствиями утечек. Указанные нововведения были отмечены в Перечне поручений Президента РФ по итогам заседания Совета по развитию гражданского общества и правам человека, прошедшего 07.12.2022 г.[13]

Из последнего в правотворческой деятельности Роскомнадзора можно отметить установление правил оценки вреда, который может быть причинен субъектам персональных данных[14]. Данные правила позволяют определить степень вероятного вреда, что отражается в соответствующем акте об утечке. Безусловно, это способно повлиять на размеры возмещений вреда и практику их применения, однако не следует забывать, что ключевым в рассматриваемой сфере должно выступать предотвращение причинения вреда субъектам ввиду утечек персональных данных и действенные механизмы по снижению причиненного вреда. Так, интересным представляется предложение о минимальных размерах оборотного штрафа операторам, компенсировавшим вред от утечки персональных данных большинству пострадавших[15].

Подходы в доктрине к разрешению ситуации с киберугрозами

Некоторые подходы в доктрине отличаются тем, что исследователи акцентируют внимание не на мерах ответственности, а на мерах защиты, которые позволят предотвратить или прекратить утечки персональных данных. Указывается, что пользователи зачастую самостоятельно передают через смартфоны и персональные компьютеры персональные данные, которые могут быть использованы в том числе в противоправных целях иными лицами. То есть необходимо пользователям быть бдительнее, знать о своих правах и правовых последствиях. Даются в том числе комментарии использовать антивирусные программы и не скачивать с сомнительных сайтов любые данные, что могло бы привести к утечке персональных данных [3, с. 92, 95]. Действительно, с данным подходом следует согласиться. В данном смысле упор делается на необходимость принятия субъектами персональных данных своего рода мер самозащиты, что позволяет обеспечить сохранность собственных персональных данных.

В литературе делается следующий неутешительный вывод о том, что в настоящее время человек, даже не осознавая этого, ежеминутно предоставляет огромное количество информации о себе самым различным компаниям. При этом мельчайшие частицы такой информации могут воссоздать полный образ человека [4, с. 150–152]. Как замечается, чем больше персональных данных о лице собирается и обрабатывается, тем выше риски нарушения его прав на защиту персональных данных [5, с. 52]. Все это выступает предпосылками утечек персональных данных и порождает проблемы в правоприменении.

---

[12] Общий регламент защиты персональных данных (GDPR) Европейского союза. GDPR TEXT. URL: https://gdpr-text.com/ru/ (дата обращения: 05.06.2023).

[13] Перечень поручений Президента РФ по итогам заседания Совета по развитию гражданского общества и правам человека. 12.01.2023 // СПС «КонсультантПлюс».

[14] Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27.10.2022 № 178 «Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных» // СПС «Гарант».

[15] Компенсация пострадавшим от утечек данных смягчит наказание для компаний. РБК. Технологии и медиа. 29 ноября 2022 г. URL: https://www.rbc.ru/technology_and_media/29/11/2022/638499da9a79473a5b92a52d (дата обращения: 03.06.2023).

Другой автор, В. В. Архипов, верно указывает, что помочь борьбе с нарушениями персональных данных поможет их признание не товаром, как указывается некоторыми в доктрине [6, с. 158–159], а именно нематериальным благом [7]. М. А. Рожкова, отмечая существование концепции персональных данных как товара [8, с. 281], замечает, что если персональные данные не обезличены (п. 9 ст. 3, ч. 7 ст. 5, п. 9 ч. 1 ст. 6 Закона о персональных данных), то они не могут использоваться в гражданском обороте. А уже большие данные, включающие в себя обезличенные персональные данные, могут быть объектом гражданско-правовых сделок [9].

В. И. Солдатова, отмечая в целом проблему незащищенности персональных данных граждан от несанкционированного доступа неограниченного круга лиц [10], приходит к тому, что имеющиеся средства защиты персональных данных являются недостаточными в условиях использования цифровых технологий, необходимо усиление ответственности. Разночтения у правоприменителей вызывает и отнесение к персональным данным конкретной информации о физических лицах. Необходимым является определение критериев, по которым те или иные сведения о лице можно относить к персональным данным [11, с. 41]. В то же время, судебная практика сама достаточно успешно формулирует критерии отнесения той или иной информации к персональным данным (так, например, данные, оставленные физическими лицами в социальных сетях «ВКонтакте», «Одноклассники», «Мой мир», Instragram (запрещено в РФ), Twitter; на интернет-порталах «Авито», «Авто.ру» и др., рассматриваются как персональные данные)[16]. Об этом же пишет в своей статье А. Балдынова, указывая, что круг персональных данных необходимо очерчивать очень полно [12, с. 23, 24], в этом плане правоприменительная практика так же, как правило, исходит из принципа максимального расширения перечня персональных данных, если они позволяют идентифицировать то или иное физическое лицо. Расширяя средства правовой защиты, суды при рассмотрении дел об использовании персональных данных граждан применяют нормы Закона РФ «О защите прав потребителей».

Авторский подход к решению проблемы

Исходя из анализа законодательства и правоприменительной практики, делаем вывод, что мало перечисления прав, важны гарантии в киберсфере через реализацию безопасности персональных данных в киберсреде путем использования соответствующих мер защиты. Представляется, что в сложившейся ситуации необходимо внедрить соответствующие превентивные меры, которые бы позволили априори минимизировать утечки персональных данных пользователей. Такими мерами может выступать комплаенс, позволяющий технически и юридически выявить имеющиеся риски безопасности персональных данных, нарушения оператором тех или иных законодательных положений, доступ третьих лиц к персональным данным и т. д. Кроме того, сотрудники должны на постоянной основе обучаться основам безопасного управления персональными данными, понимать, в чем заключается неправомерное использование персональных данных и не допускать этого.

Кроме того, необходим, безусловно, и постконтроль, заключающийся в проведении проверки деятельности оператора на предмет нарушений, приведших к утечке персональных данных. Правоприменительный орган (Роскомнадзор) может выявить, что послужило точной причиной утечки персональных данных и как можно ее предотвратить на будущее время. Только комплексный подход, заключающийся и в предотвращении наступления вреда, и в оценке деятельности оператора на предмет наличия нарушений, способен изменить текущую ситуацию с оборотом персональных данных.

[16] См.: Определение Верховного Суда Российской Федерации от 29.01.2018 № 305-КГ17-21291 по делу № А40-5250/2017, Постановление Девятого арбитражного апелляционного суда от 27.07.2017 № 09АП-31744/2017 по делу № А40-5250/17.

Заключение

Рассматривая настоящий этап цифровизации права Российской Федерации, нельзя не отметить, что персональные данные стали новым золотом, законодательства стран устанавливают, какая информация считается персональными данными, а также определяют ответственность за нарушения в указанной сфере. Однако существует неурегулированный пробел, связанный с определением утечки персональных данных и мер по ее предотвращению и минимизацией возникших последствий. В доктрине поднимаются вопросы о том, насколько конкретно и полно очерчен круг персональных данных, о необходимости усиления мер ответственности, закреплении оборотных штрафов. Нам видится, что необходимо не только минимизировать последствия утечек и стимулировать операторов к соблюдению законодательства о персональных данных путем усиления мер ответственности, но и предотвратить и ликвидировать причины утечек персональных данных. Указанное будет содействовать уменьшению числа утечек персональных данных в Российской Федерации и минимизации негативных последствий государства, бизнеса и общества.

Список литературы

1. **Росиков А.** Согласие на распространение персональных данных: новые требования // Кадровая служба и управление персоналом предприятия. 2021. № 6 // СПС «КонсультантПлюс».
2. **Савельев А. И.** Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд., перераб. и доп. М.: Статут, 2021 // СПС «КонсультантПлюс».
3. **Барков А. В., Киселев А. С.** Правовое обеспечение информационной безопасности: инструменты противодействия киберугрозам // Журнал прикладных исследований. Право. 2022. С. 91–96.
4. **Грибанов А. А.** Общий регламент о защите персональных данных (General Data Protection Regulation): идеи для совершенствования российского законодательства // Закон. 2018. № 3. С. 149–162.
5. **Савельев А. И.** Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал Высшей школы экономики. 2015. № 1. С. 43–66.
6. **6. Нохрина М. Л.** Понятие и признаки нематериальных благ: законодательство и цивилистическая наука // Известия высших учебных заведений. Правоведение. 2013. № 5. С. 143–160.
7. **7. Архипов В. В.** Проблема квалификации персональных данных как нематериальных благ в условиях цифровой экономики, или Нет ничего более практичного, чем хорошая теория // Закон. 2018. № 2. С. 52–68.
8. **Рожкова М. А., Глонина В. Н.** Персональные и неперсональные данные в составе больших данных // Право цифровой экономики. 2020. Ежегодник-антология. Сер. :Анализ современного права / IP & Digital Law / рук. и науч. ред. М. А. Рожкова. М.: Статут, 2020. С. 271–296.
9. **Урошлева А.** Коммерциализация персональных данных и понятие «биг дата» – злободневные вопросы IT-сферы. Гарант.ру. Новости и аналитика. Аналитические статьи. 22 ноября 2018. URL: https://www.garant.ru/article/1229761/
10. **Солдатова В. И.** Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. № 2. С. 33–43.

11. **Солдатова В. И.** Новые законодательные меры по защите персональных данных // Право и экономика. 2023. № 3 // СПС «КонсультантПлюс».
12. **Балдынова А.** Персональные данные // Административное право. 2020. № 4. С. 23-24.

References

1. **Rosikov A.** Soglasie na Rasprostranenie Personal'nyh Dannyh: Novye Trebovaniya [Consent to the Dissemination of Personal Data: New Requirements], *Kadrovaya Sluzhba i Upravlenie Personalom Predpriyatiya*, 2021, vol. 6. SPS «Konsul'tantPlyus». (in Russ.)
2. **Savel'ev A. I.** Nauchno-Prakticheskij Postatejnyj Kommentarij k Federal'nomu Zakonu «O Personal'nyh Dannyh» [Scientific and Practical Article-by-Article Commentary on the Federal Law "On Personal Data"]. 2-e izd., pererab. i dop. Moscow, Statut, 2021. SPS «Konsul'tantPlyus». (in Russ.)
3. **Barkov A. V., Kiselev A. S.** Pravovoe Obespechenie Informacionnoj Bezopasnosti: Instrumenty Protivodejstviya Kiberugrozam [Legal Support of Information Security: Tools to Counter Cyber Threats], *Zhurnal Prikladnyh Issledovanij, Pravo*, 2022, pp. 91–96. (in Russ.)
4. **Gribanov A. A.** Obshchij Reglament o Zashchite Personal'nyh Dannyh (General Data Protection Regulation): Idei dlya Sovershenstvovaniya Rossijskogo Zakonodatel'stva [General Data Protection Regulation: Ideas for Improving Russian Legislation], *Zakon*, 2018, vol. 3, pp. 149–162. (in Russ.)
5. **Savel'ev A. I.** Problemy Primeneniya Zakonodatel'stva o Personal'nyh Dannyh v Epohu «Bol'shih Dannyh» (Big Data) [Problems of Application of Legislation on Personal Data in the Era of "Big Data"], *Pravo. Zhurnal Vysshej shkoly ekonomiki*, 2015, vol. 1, pp. 43–66. (in Russ.)
6. **Nohrina M. L.** Ponyatie i Priznaki Nematerial'nyh Blag: Zakonodatel'stvo i Civilisticheskaya Nauka [The Concept and Signs of Intangible Benefits: Legislation and Civil Science], *Izvestiya Vysshih Uchebnyh Zavedenij. Pravovedenie*, 2013, vol. 5, pp. 143–160. (in Russ.)
7. **Arhipov V. V.** Problema Kvalifikacii Personal'nyh Dannyh kak Nematerial'nyh Blag v Usloviyah Cifrovoj Ekonomiki, ili Net Nichego Bolee Prakticheskogo, Chem Horoshaya Teoriya [The Problem of Qualifying Personal Data as Intangible Goods in the Digital Economy, or there is Nothing More Practical than a Good Theory], *Zakon*, 2018, vol. 2, pp. 52–68. (in Russ.)
8. **Rozhkova M. A., Glonina V. N.** Personal'nye i Nepersonal'nye Dannye v Sostave Bol'shih Dannyh [Personal and Non-Personal Data as Part of Big Data]. Pravo Cifrovoj Ekonomiki 2020. Ezhegodnik-Antologiya. Ser. «Analiz Sovremennogo Prava / IP & Digital Law», ruk. i nauch. red. M.A. Rozhkova. Moscow, Statut, 2020. Pp. 271–296. (in Russ.)
9. **Uroshleva A.** Kommercializaciya Personal'nyh Dannyh i Ponyatie «Big Data» - Zlobodnevnye Voprosy IT-Sfery [Commercialization of Personal Data and the Concept of "Big Data" are Topical Issues in the IT Sphere]. Garant.ru. Novosti i Analitika. Analiticheskie Stat'i. 22 November, 2018. URL: https://www.garant.ru/article/1229761/.
10. **Soldatova V. I.** Zashchita Personal'nyh Dannyh v Usloviyah Primeneniya Cifrovyh Tekhnologij [Protection of Personal Data in the Context of the Use of Digital Technologies], *Lex russica*, 2020, vol. 2, pp. 33–43. (in Russ.)
11. **Soldatova V. I.** Novye Zakonodatel'nye Mery po Zashchite Personal'nyh Dannyh [New Legislative Measures to Protect Personal Data], *Pravo i ekonomika*, 2023, vol. 3. SPS «Konsul'tantPlyus».
12. **Baldynova A.** Personal data // Administrative Law. 2020. № 4. P. 23–24. (in Russ.)

Информация об авторе

Елизавета Владимировна Зайнутдинова, кандидат юридических наук

Information about the Author

Elizaveta V. Zainutdinova, Ph.D in Law

Статья поступила в редакцию 09.06.2023;
одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 09.06.2023;
approved after reviewing 21.06.2023; accepted for publication 31.07.2023

Научная статья

УДК 347.121.2
DOI 10.25205/2542-0410-2023-19-3-47-56

Проблемы защиты персональных данных в условиях цифровой трансформации

Яна Александровна Карунная

Новосибирский государственный университет
Новосибирск, Россия

advokat2631@bk.ru

Аннотация

В статье представлен анализ отечественного законодательства, регламентирующего защиту персональных данных; рассмотрены проблемы защиты персональных данных в условиях усиления роли цифровых ресурсов, использования технологии трекинга и цифровых технологий, позволяющих фиксировать, осуществлять сбор и обрабатывать персональные данные физических лиц; аргументирована необходимость разрабатывать современные эффективные методы, технические средства обнаружения и предотвращения несанкционированного использования персональных данных, а также потребность в обсуждении и последующей корректировке дополнительной правовой регламентации института защиты персональных данных, в частности, отдельных положений закона.

Ключевые слова

цифровые технологии, искусственный интеллект, системы видеонаблюдения, персональные данные, биометрические данные, big data

Для цитирования

Карунная Я. А. Проблемы защиты персональных данных в условиях цифровой трансформации // Юридическая наука и практика. 2023. Т. 19, № 3. С. 47–56. DOI 10.25205/2542-0410-2023-19-3-47-56

Problems of Personal Data Protection in the Context of Digital Transformation

Yana A. Karunnaya

Novosibirsk State University,
Novosibirsk, Russia

advokat2631@bk.ru

Abstract

The article presents an analysis of domestic legislation regulating the protection of personal data; the problems of personal data protection in the context of increasing the role of digital resources, the use of tracking technology and digital technologies that allow recording, collecting and processing personal data of individuals are considered; the argumentation is given to substantiate the need to develop modern effective methods, technical means of detecting and preventing unauthorized use of personal data, additional legal regulation of the institute of personal data protection, and certain provisions of the law – in discussion and subsequent correction.

Keywords

Digital technologies, artificial intelligence, video surveillance systems, personal data, biometric data, Big data

For citation

Karunnaya Ya. A. Problems of personal data protection in the context of ligital transformation. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 47–56. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-47-56

Резкое ускорение трансформирующих изменений в сфере информатики и цифровых технологий предопределило вектор развития общественных отношений в условиях цифровизации. Цифровая трансформация – одна из целей развития Российской Федерации до 2030 г., в соответствии с которой ориентир направлен на следующие целевые показатели: достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы, в том числе здравоохранения и образования, а также государственного управления; увеличение доли массовых социально значимых услуг, доступных в электронном виде, до 95 %; рост доли домохозяйств, которым обеспечена возможность широкополосного доступа к информационно-телекоммуникационной сети «Интернет», до 97 %; увеличение вложений в отечественные решения в сфере информационных технологий в четыре раза по сравнению с показателем 2019 г.[1] В соответствии со Стратегией цифровой трансформации, в регионах, в том числе в Новосибирской области, для обеспечения государственного управления, развития экономики и социальной сферы внедряются следующие технологи: «нейротехнологии и искусственный интеллект; технологии беспроводной связи и промышленный интернет вещей IoT; новые производственные технологии, в том числе технология «цифровой двойник»; системы распределенного реестра; технологии виртуальной и дополненной реальности»[2]. Цифровая трансформация повлекла за собой масштабное использование персональных данных, в связи с чем для проведения комплекса значимых реформ в Российской Федерации особое значение приобретают вопросы разработки эффективного правового регулирования отношений для защиты данных, составляющих персональную информацию граждан. Отечественное законодательство в результате его реформирования совершенствуется. Тем не менее следует констатировать, что практика использования современных технологий, в том числе доступа к информации посредством онлайн-сервисов, распространяется более быстрыми темпами, в сравнении с разработкой комплекса технических средств и положений, направленных на обеспечение механизма, с помощью которого можно было максимально надежно обеспечить защиту персональных данных и предотвратить несанкционированное вторжение в сферу личной жизни граждан.

Актуальными представляются вопросы защиты личных данных в условиях повсеместного применения технологии трекинга, цифровых технологий, используемых для машинного обучения и хранения больших объемов информации (big data).

Для целей настоящего исследования под использованием технологии трекинга понимается практика размещения видеокамер наблюдения – начиная от их размещения в домофонах многоквартирного дома, при входе и внутри помещений сферы обслуживания, образовательных, медицинских и иных учреждений, местах парковки, светофорах, вдоль дорог и др., заканчивая камерами в аэропортах и вокзалах. Современные системы наблюдения позволяют отследить передвижения практически каждого человека. По данным TelecomDaily, Россия занимает второе место по темпу роста видеонаблюдения за гражданами, число видеокамер в общественных местах за год выросло на 10 %. В первой половине 2021 г. число камер, установленных

---

[1] О национальных целях развития Российской Федерации на период до 2030 года: Указ Президента Российской Федерации от 21.07.2020 № 474 // Собрание законодательства Рос. Федерации. 2018. № 20. Ст. 2817; № 30. Ст. 4717.

[2] Стратегия цифровой трансформации ключевых отраслей экономики, социальной сферы и государственного управления Новосибирской области, утв. постановлением губернатора от 31.08.22 №161 // Официальный интернет-портал правовой информации Новосибирской области: https://pravo.nso.ru (дата обращения: 05.06.2023).

в парках, на улицах, вокзалах, магазинах, превысило 15 млн штук. По количеству работающей техники видеонаблюдения РФ уже на третьем месте после Китая, где на октябрь 2021 г. работают 200 млн видеокамер[3]. В настоящее время в России реализуются мероприятия по массовому производству IP-камер видеонаблюдения в соответствии планом, предусмотренным дорожной картой развития высокотехнологичного направления (области) «Новое индустриальное программное обеспечение» на период до 2030 г.[4] При этом в результате расширения технических возможностей систем видеонаблюдения появилась возможность распознавать и идентифицировать лица, в том числе в плотном потоке людей. Такие системы применяются для фейсконтроля в различных заведениях, в целях распознавания отдельных лиц при организации системы управления доступом. С помощью IP-камеры возможно определить нахождение на территории объекта посторонних лиц, информация о которых отсутствует в базе, произвести зональное сканирование в целях поиска и опознания системой лица, занесенного в базу для допуска на объект. Распознавание осуществляется благодаря функции выбранного алгоритма, в соответствии с которым полученное отсканированное изображение лица «гостя» сравнивается с эталонными картинками, которые уже имеются в базе. Технология, используемая в IP-камере, используется для анализа потока и передачи на сервер уже обработанных данных, в соответствии с которыми определяются условия доступа на объект – доступ становится возможным или невозможным.

В условиях цифровой трансформации распространение практики использования систем видеонаблюдения неизбежно. Благодаря поддержанию систем видеонаблюдения обеспечивается общественный порядок, оперативное раскрытие правонарушений, допуск в определенные помещения лиц, имеющих разрешение на это, соблюдение правил дорожного движения, предотвращение дорожно-транспортных происшествий и др. Кроме того, записи с камер наблюдения могут иметь доказательственное значение по уголовным и гражданским делам, при установлении обстоятельств совершения административного правонарушения. Вместе с тем практика использования систем видеонаблюдения обнаруживает и некоторые проблемы, необходимость в разрешении которых настоятельна как с позиции теории, так и правоприменения. Ключевая проблема заключается в возможности накапливать (записывать) информацию, содержащую персональные данные о конкретном лице, в том числе сведения, составляющие медицинскую, адвокатскую, банковскую или иную тайну.

В соответствии со ст. 24 Конституции РФ, сбор, хранение, использование и распространение информации о частной жизни человека без его согласия не допускаются. Согласно ст. 3 Федерального закона «О персональных данных» (далее – Закон о персональных данных), персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). К такой информации Закон относит и биометрические данные, т. е. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных[5].

---

[3] Видеонаблюдение (рынок_России). URL: https://www.tadviser.ru/index.php/ (дата обращения: 10.06.2023).

[4] Распоряжение Правительства Российской Федерации от 28 декабря 2022 г. № 4263-р // Собрание законодательства Рос. Федерации. 2023. № 1 (ч. III). Ст. 424.

[5] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06.02.2023) // Собрание законодательства Рос. Федерации. 31 июля 2006 г. № 31 (часть I). Ст. 3451; Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных, а также о внесении

В ст. 152.1 ГК РФ закреплено положение, в силу которого обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображен) допускаются только с согласия этого гражданина. Такое согласие не требуется в случаях, когда: использование изображения осуществляется в государственных, общественных или иных публичных интересах; изображение гражданина получено при съемке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования; гражданин позировал за плату. Анализ положений, закрепленных в п. 1 ст. 22 и ч. 2 ст. 11 Закона о персональных данных, показывает, что все сведения, на основании которых может быть выполнена идентификация личности, приравниваются к персональным; биометрические данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных. В ст. 7 указанного Закона закреплена обязанность операторов и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных.

Важно признать, что современные системы видеонаблюдения фиксируют именно биометрические персональные данные, т. е. физиологические и биологические особенности человека, на основании которых можно установить его личность. Однако, по смыслу Закона, само по себе видеонаблюдение в общественных местах не является сбором персональных данных, в связи с чем не требует согласия субъекта персональных данных, за исключением случаев передачи записи третьим лицам или использования ее в целях установления личности человека. Таким образом, если камеры установлены для идентификации конкретного лица, например, для того чтобы он был идентифицирован через систему лояльности, то для осуществления такой записи необходимо получить согласие субъекта о персональных данных. Напротив, если речь идет об использовании систем видеонаблюдения с целью контроля обстановки, то такое использование не подпадает под действие приведенных правовых положений, так как в данном случае имеет место мониторинг ситуации с помощью камер, а не идентификация субъекта по видеозаписи на основании его биометрических данных. При регистрации неправомерных действий с помощью задействования функции видеонаблюдения установление правонарушителя может проводиться в порядке, который регламентируется процессуальным законодательством. Однако в практике имеется немало примеров, когда вопрос о границах полномочий лиц, осуществляющих проверочные мероприятия (расследование), был предметом отдельного рассмотрения. Проблема обнаруживается в случае бесконтрольного получения записей с камер видеонаблюдения и не во всех случаях для оценки их доказательственного значения, но для получения информации о конкретном лице. При этом для получения записи с камер видеонаблюдения разрешения суда не требуется. Чрезмерная экстенсивная слежка за гражданами без каких-либо ограничений (подтверждений) того, зачем ведется наблюдение, как долго оно может продолжаться, а главное – какова в дальнейшем должна быть судьба собранных материалов, несет риски утечки персональной информации и, как следствие, возникновения неблагоприятных последствий для субъекта персональных данных. Представляется, что наблюдение, в том числе использование записи, допустимо и необходимо в демократическом обществе, однако его пределы должны быть четко установлены законом, с тем чтобы защитить право граждан на неприкосновенность частной жизни. Полученные доказательства должны быть надлежащим образом задокументированы, а затем, после минования надобности, уничтожены. Принимая во внимание заметный рост киберпреступлений, риск несанкционированного использования информации, содержащей персональные данные, достаточно велик.

изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 12.07.2022) // Собрание законодательства РФ. 2018. № 28. Ст. 4234.

Гарантий, что персональная информация, равно как сведения о личной жизни, не будет несанкционированно использована, – нет. К тому же изначально информация может быть получена на законных основаниях. Вместе с тем при предоставлении информации с камер видеонаблюдения, как правило, не всегда возможно вычленить сведения относительно конкретного лица. Зачастую в объектив камеры по воле случая попадают и другие лица, не являющиеся фигурантами, т. е. лицами, в отношении которых оперативных, следственных и иных мероприятий не проводится. Такие «случайные» лица могут не догадываться о том, что информация о них, например, наличествует в материалах уголовного, административного или гражданского дела, могут не знать о том, что их персональные данные фигурируют в материалах служебной проверки (служебного расследования), но при этом доступ к этим материалам может иметь не только гражданин, в отношении которого проводилась проверка (расследование), обвиняемый и его защитник, но и потерпевший, стороны по делу и иные лица, участвующие в деле (их представители), эксперт и др. Например, распространена практика, когда для подтверждения информации о передвижения конкретного гражданина, в отношении которого проводятся проверочные мероприятия (расследование), запрашивается запись с камер видеонаблюдения, фиксирующих обстоятельства его нахождения в конкретном месте, участия в каких-либо мероприятиях, где одновременно могут находиться его друзья, родственники или иные лица, в отношении которых указанные мероприятия не проводятся. Запись с камеры видеонаблюдения может зафиксировать факты обращения гражданина за медицинской или правовой помощью. Информация, зафиксированная камерами видеонаблюдения, установленными в местах общего пользования, предоставляется собственникам многоквартирного дома для установления каких-либо обстоятельств. Например, есть практика, когда для установления лиц, причастных к порче общедомового имущества, просматриваются записи, фиксирующие отдельных лиц, не причастных к устанавливаемым обстоятельствам. При таких обстоятельствах основания считать, что информация о передвижениях, встречах, знакомствах, отношениях и др. может стать известной третьим лицам или окажется составной частью досье на человека, довольно весомые. При этом установить лицо, распространившее такие сведения или их накапливающее, сложно. Кроме того, работоспособность систем видеонаблюдения, как правило, поддерживается коммерческими организациями, репутация которых в обеспечении защиты сведений, составляющих персональные данные, небезупречна.

Приведенные обстоятельства указывают на то, что нормативные положения, включая норму ст. 7 Закона о персональных данных, носят скорее дискретный характер и не обеспечивают должный уровень защищенности.

Следующая важная проблема – обеспечение механизма защиты данных в процессе их сбора и обработки с использованием цифровых технологий и для усовершенствования цифровых технологий, в том числе для обучения искусственного интеллекта. Например, с целью выполнения задачи распознавания физического лица обрабатывается большой массив информации, в том числе той, которая содержит персональные данные. В частности, в целях машинного обучения исследуются и анализируются параметры готовых образов и на основании полученных данных с помощью технологии искусственного интеллекта становится возможным определить пол, возраст, индивидуальные особенности человека. Сфера использования таких технологий обширна. Видеокамеры могут быть установлены в рекламных баннерах, и тот, кто знакомится с рекламной информацией, не знает, что его изображение может быть зафиксировано и использовано для определения, к примеру, круга потребителей, заинтересовавшихся рекламной информацией. С. М. Пястолов определяет целевую рекламу как прием, который «увеличивает вероятность покупки или определенных действий потребителя. Чтобы добиться этого, компании собирают данные о поведении своих потребителей или покупают кейсы и применяют методы машинного обучения, чтобы прогнозировать модели будущего потребительского поведения» [1, с. 87]. С помощью нейронных сетей возможно получить качественное распознавание отдельных лиц при минимальных временных затратах. Многослойное сканирование лица позво-

ляет определить соответствие полученного изображения с тем, которое имеется в базе данных. Однако для статистического сравнения полученных изображений с теми эталонами, которые внесены в базу, необходимо машинное обучение, в результате которого система способна учесть антропометрические точки, наиболее ярко характеризующие человека, в том числе высоту и ширину лба, линию положения глазной щели, ширину спинки носа, высоту верхней губы, ушной раковины и др. Таким образом, с помощью «умной системы», в том числе для ее совершенствования, сканируются и обрабатываются изображения разных лиц, которые даже не подозревают, что их биометрические данные могут использоваться и храниться. Более того, технологический процесс обусловливает необходимость пополнения базы новыми эталонами и образцами для их статистики, сравнения и исследования для более точного определения биометрических параметров. Разработка систем распознавания лиц в настоящее время востребована, следовательно, со временем будет только совершенствоваться. Так, в онлайн-презентации новой версии Macroscop 4.1 демонстрируются возможности модуля распознавания лиц, которые обеспечивают высокую точность распознавания лиц. Заявляется, что важным применением модуля может быть автоматическая идентификация гостей отеля, клиентов ресторана, а также посетителей других подобных предприятий. При этом указывается, что для работы с модулем необходимо загрузить базу данных лиц или добавить лица из видеоархива в ПО Macroscop. База данных лиц может содержать фотографии или скриншоты с лицами людей. К изображениям можно добавлять имена, фамилии и любые комментарии, а также добавлять фотографии в такие списки, как VIP-клиенты, нежелательные посетители и др. В качестве эталонного изображения используется цифровое изображение, предварительно загруженное в базу данных лиц модуля, или изображение, снятое камерой системы на контрольно-пропускном пункте, оборудованном системой видеонаблюдения. При работе с видеоархивом можно фильтровать все события по фотографии человека. Таким образом, возможно найти все события, произошедшие с конкретным человеком, а также увидеть, где находился этот человек и что он делал[6].

Венчурная студия Synesis, работающая над проектами в области умных городов, ПО для организации мероприятий, мессенджеров и онлайн-казино, заявляет о разработке Kipod, которая помогает всем – от правоохранительных органов, государственных и общественных организаций безопасности до частных служб безопасности и коммерческих структур – извлекать выгоду из больших массивов видеоданных. Уникальная облачная платформа обеспечивает мгновенный поиск видеоконтента и непрерывный мониторинг событий по миллионам камер, обслуживая при этом миллионы пользователей на любом устройстве. Задействование искусственного интеллекта дает следующие возможности: идентификация личности, обнаружение внештатных ситуаций, аудиоаналитика, идентификация автомобилей, межкамерное слежение, классификация объектов big data, глобальный поиск по тысячам мест, фасетные фильтры, неограниченные списки поиска людей и транспортных средств. Kipod производит практически в режиме момента поиск в огромном количестве данных. Задействованные алгоритмы позволяют идентифицировать конкретного человека. В результате возможно определить местонахождение человека и время его нахождения в определенном месте. С помощью заявленных функций обнаружение человека возможно также и без его фотографии при имеющихся других данных, таких как пол, раса, возраст и др. С помощью технологии Big Data API можно наблюдать общую картину того, что происходит в городе, посчитать людей и транспортные средства, используя стандартные камеры видеонаблюдения, заявляется на сайте компании[7].

Умное видеонаблюдение с применением технологии распознавания лиц планомерно интегрируется практически во все города. На основе биометрических данных граждан создаются

[6] Онлайн-презентация новой версии Macroscop 4.1 «Распознавание лиц Light». URL: https://macroscop.com/produkty/programma-dlya-ip-kamer/raspoznavanie-lic (дата обращения: 05.07.2023).

[7] Интернет-сайт kipod.com // URL: https://kipod.com/ru/features (дата обращения: 08.07.2023).

базы фотографий лиц со статусами «доверенное» и «черный список». Без специальных исследований и обучения искусственного интеллекта на основе конкретных изображений это было невозможно. По общему правилу, закрепленному в ч. 3 ст. 18 Закона о персональных данных, если персональные данные получены не от субъекта персональных данных, оператор до начала обработки таких персональных данных обязан предоставить субъекту персональных данных информацию относительно наименования либо фамилии, имени, отчества и адреса оператора или его представителя; цели обработки персональных данных и ее правового основания; перечня персональных данных; предполагаемых пользователей персональных данных; источника получения персональных данных. Однако, в силу ч. 4 приведенной нормы, оператор освобождается от обязанности предоставить субъекту персональных данных перечисленную информацию, если осуществляет обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных. При таком нормативном исключении возникает вопрос о правомерности использования персональных данных в процессе проведения различного рода исследований для обучения искусственного интеллекта, равно как и объеме самих исследований, а также пределах использования полученных результатов.

Таким образом, следует констатировать, что цифровая трансформация повлекла за собой масштабное использование персональных данных, которые стали одной из составляющих big data. Рассматривая в ретроспективе замысел big data, можно проследить определенный процесс его эволюции. В литературе отмечается, что «в начале 2000-х годов он стал определяться как модель 3V: объем (volume), скорость (velocity) и вариативность (variety). Эта модель эволюционировала, приспосабливаясь к новой цифровой реальности, и превратилась в модель 4V: был добавлен такой параметр, как ценность (value) – процесс извлечения ценной информации из набора данных, известный как «аналитика больших данных». В настоящее время большие данные чаще определяют уже в терминах модели 5V, в которую добавлен параметр достоверности (veracity), означающий адекватное управление данными и соблюдение права на частную жизнь» [2, с. 53]. Поскольку «в сущности, понятие Big Data подразумевает работу с информацией огромного объема и разнообразного состава, которая часто обновляется и может располагаться в различных информационных источниках» [3, с. 320], вопрос относительно целей использования аккумулируемой информации лицами, владеющими ею, оказывается непростым. М. О. Лихачев справедливо акцентирует внимание на том, «сбор данных «ведет к тотальной «датафикации»: наблюдению и сбору данных о происходящих процессах, поведении людей и взаимосвязях, возникающих между ними. Практически любая активность в Интернете в настоящее время – это основа для формирования баз данных, которые не просто являются информацией, отражающей реальный мир, а используются для того, чтобы воздействовать на него, изменять его в интересах тех, кто владеет этой информацией» [4, с. 73].

Совершенствование технологий, позволяющих собирать различные данные и предоставляющие возможность персонифицировать людей с использованием биометрических данных, индивидуальных особенностей, деятельности и т. д., влечет за собой серьезные риски утечки информации, составляющей персональные сведения. При этом возможность трансграничной передачи таких сведений, а также наличие инновационных разработок, предлагающих сходные решения, но контролируемые разными разработчиками и компаниями, затрудняет установление лиц, ответственных за утечку персональных данных либо делает это невозможным. Как показывает практика, предупредительные меры оказываются недейственными. Так, по мнению экспертов InfoWatch, «в России за год утекло более 667 млн записей с персональными данными – это в 4,5 раза больше населения страны… По подсчетам Group-IB, количество утекших записей в прошлом году в десять раз превысило население России: строчки включают имена клиентов, их телефоны, адреса, даты рождения, а в некоторых можно найти хеш-пароли, паспортные данные, подробности заказов и другую чувствительную информа-

цию. Общее количество строк данных пользователей в утечках в 2022 году составило 1,4 млрд, для сравнения: в 2021 году их насчитывалось всего 33 млн»[8]. Отток информации имел место в самых различных сферах: финансовой, энергетической, промышленной, строительной, транспортной, развлекательной, образовательной, страховой, IT-компаний, сервиса доставки, онлайн-обслуживания и др. [9]

По мнению В. К. Шайдулиной, «В настоящее время, когда сбор информации о пользователях обладает массовым характером, даже самый безобидный фрагмент подобных сведений, будучи соединенным с другим, способен дать гораздо больше данных о человеке, чем его анкета. Значительные массивы сведений о пользователях, циркулирующие в цифровой форме, привели к возникновению за рубежом новых игроков на информационном рынке. В частности, появились информационные брокеры, которые на основе стекающихся к ним из разных интернет-сервисов данных, составляют детальные профайлы людей и предоставляют к ним доступ заинтересованным субъектам» [5, с. 4].

Несмотря на определенную нормативную обеспеченность защиты персональных данных, в современной действительности именно потребитель (пользователь приложения) при оказании услуги или приобретении товара, раскрывая информацию о себе и соглашаясь на ее обработку, несет риск возникновения негативных последствий от их использования. При этом масштабное распространение цифровых технологий в практическом плане зачастую не дает потребителю (пользователю) возможности выбора – не дал согласие на обработку – не получил услугу или доступ к приложению. Вместе с тем получение сведений, составляющих определенных объем персональных данных, не всегда необходимо для работы приложения, оказания услуги или выполнения работы. Представляется, что учитывая коммерческую составляющую клиентской базы, сбор персональных данных может осуществляется целенаправленно, при этом, соглашаясь на обработку данных, гражданин (потребитель) не имеет гарантий и уверенности, что они будут использованы по декларируемому назначению, следовательно, в принципе не может предотвратить риск наступления неблагоприятных последствий от несанкционированного использования его данных. Акцентируя внимание на вопросе влияния проблемы персональных данных на этику искусственного интеллекта, доктор философских наук Н. А. Ястреб приходит к обоснованному выводу: «Парадокс информированного согласия состоит в том, что без специальных знаний и владения цифровыми навыками на высоком уровне человек не может быть информирован о том, согласие на что он дает. Поскольку в реальности практически никто из пользователей не в состоянии спрогнозировать, какие именно данные о нем получит система искусственного интеллекта и как они могут быть использованы, то совершенно точно можно утверждать, что права человека нарушаются. Особенно это касается тех случаев, когда человек не может по объективным причинам отказаться от взаимодействия с искусственным интеллектом, например, если речь идет о медицинском реанимационном оборудовании или системах отслеживания нарушителей карантина. Согласие в этом случае, будучи формально добровольным, фактически является вынужденным» [6, с. 12].

Проблема защиты персональных данных осложняется и тем, что полный перечь согласий, уже выданных гражданином, составить затруднительно. Следовательно, отследить, проконтролировать и «управлять» своими личными данными в практическом плане крайне затруднительно или невозможно.

Таким образом, в условиях цифровой трансформации общественных отношений, когда обнаруживаются новые способы взаимодействия человека и искусственного интеллекта, тре-

[8] В России за год утекло более 660 млн записей с персональными данными // Подробнее на РБК: https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c (дата обращения: 10.07.2023).

[9] Сливной год: злоумышленники выложили 1,4 млрд строк из утекших баз российских компаний. URL: https://www.facct.ru/media-center/press-releases/database-2022/

бующие адекватной интерпретации в правоприменительной практике, учитывая возможность трансграничного распространения персональных данных, рамки существующих и ожидаемых параметров правовой системы диктуют необходимость поиска оптимального варианта обеспечения защиты личной информации граждан. Ввиду неизбежности процесса внедрения цифровых технологий приоритетным направлением следует признать разработку современных эффективных методов, технических средств обнаружения и предотвращения несанкционированного использования данных, содержащих персональную информацию. Учитывая необходимость максимального информирования конкретного субъекта об использовании его личных данных, обработка персональных данных для статистических или иных исследовательских целей не должна наличествовать в списке исключений, предусмотренном ч. 4 ст. 18 Закона о персональных данных, поскольку заявленные цели не исключают использование личных данных и их хранение, в том числе в целях усовершенствования технологии искусственного интеллекта, посредством которой даже обезличенные персональные данные могут быть со временем идентифицированы. С учетом приведенной аргументации видится целесообразным корректировка подп. 4 ст. 18 Закона о персональных данных.

Список литературы

1. **Пястолов С. М.** Экономические и социальные ценности, риски и организационные парадоксы больших данных: обзор // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Е. Г. Гребенщикова. М., 2019. 193 с.
2. **Виноградова Т. В. Реферат. Бласкес Д., Доменеч Х.** Источники и методы изучения больших данных для социального и экономического анализа // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Гребенщикова Е. Г. М., 2019. 193 с.
3. **Менщиков А. А., Перфильев В. Э., Федосенко М. Ю., Фабзиев И. Р.** Основные проблемы использования больших данных в современных информационных системах // Столыпинский вестник. 2022. №1. С. 316–329. URL: https://cyberleninka.ru/article/n/osnovnye-problemy-ispolzovaniya-bolshih-dannyh-v-sovremennyh-informatsionnyh-sistemah/viewer (дата обращения: 02.07.2023).
4. **Лихачев М. О.** Реферат Ж. Садовский. Данные как каптал: датафикация, аккумулирование и извлечение // Большие данные в социальных и гуманитарных науках: Сб. обзоров и рефератов / РАН. ИНИОН. Центр науч.-информ. исслед. по науке, образованию и технологиям; отв. ред. Гребенщикова Е. Г. М., 2019. 193 с.
5. **Шайдулина В. К.** Большие данные и защита персональных данных: основные проблемы теории и практики правового регулирования. 2019. С. 1-5. URL: https://cyberleninka.ru/article/n/bolshie-dannye-i-zaschita-personalnyh-dannyh-osnovnye-problemy-teorii-i-praktiki-pravovogo-regulirovaniya/viewer. (дата обращения: 10.07.2023).
6. **Ястреб Н. А.** Как проблема персональных данных меняет этику искусственного интеллекта? // Философские проблемы информационных технологий и киберпространства. 2020. № 1 (17). С. 1–16. URL: https://cyberleninka.ru/article/n/kak-problema-personalnyh-dannyh-menyaet-etiku-iskusstvennogo-intellekta/viewer.

References

1. **Pyastolov S. M.** Economic and social values, risks and organizational paradoxes of big data: a review // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION.

Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
2. **Vinogradova T. V. Abstract. Blaskes D., Domenech H.** Sources and methods of studying big data for social and economic analysis // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION. Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
3. **Menshchikov A. A., Perfiliev V. E., Fedosenko M. Yu., Fabziev I. R.** The main problems of using big data in modern information systems // Stolypin Bulletin. 2022. No. 1. Pp. 316–329. URL: https://cyberleninka.ru/article/n/osnovnye-problemy-ispolzovaniya-bolshih-dannyh-v-sovremennyh-informatsionnyh-sistemah/viewer (accessed: 02.07.2023).
4. **Likhachev M. O.** Abstract Zh. Sadovsky. Data as a captal: datafication, accumulation and extraction // Big data in the social and human sciences: Sat. reviews and abstracts / RAS. INION. Center for Scientific Information researched in science, education and technology; open ed. Grebenshchikova E. G. M., 2019. 193 p.
5. **Shaidulina V. K.** Big data and personal data protection: the main problems of theory and practice of legal regulation. URL: https://cyberleninka.ru/article/n/bolshie-dannye-i-zaschita-personalnyh-dannyh-osnovnye-problemy-teorii-i-praktiki-pravovogo-regulirovaniya/viewer. 2019. pp.1-5 (accessed: 10.07.2023).
6. **Yastreb N. A.** How does the problem of personal data change the ethics of artificial intelligence? // Philosophical problems of information technologies and cyberspace. 2020. No.1(17). Pp. 1–16. URL: https://cyberleninka.ru/article/n/kak-problema-personalnyh-dannyh-menyaet-etiku-iskusstvennogo-intellekta/viewer.

Информация об авторе

Яна Александровна Карунная, кандидат юридических наук

Information about the Author

Yana A. Karunnaya, PhD in Law

Статья поступила в редакцию 11.07.2023;
одобрена после рецензирования 21.07.2023; принята к публикации 31.07.2023

The article was submitted 11.07.2023;
approved after reviewing 21.07.2023; accepted for publication 31.07.2023

Научная статья

УДК 347.1
DOI 10.25205/2542- 0410-2023-19-3-57-68

Способы получения согласия субъекта персональных данных на их обработку в процессе организации образовательных онлайн-курсов

Дмитрий Валерьевич Пятков
Алия Рустемовна Сулейменова

Алтайский государственный университет
Барнаул, Россия

pitkov@yandex.ru

Аннотация

Авторы на примере из своей педагогической практики рассматривают частный случай получения и оформления согласия субъекта персональных данных на обработку персональных данных. В качестве примера взяты отношения между образовательной организацией и слушателями онлайн-курсов повышения квалификации. Авторы показывают проблемы, с которыми они столкнулись как организаторы образовательной деятельности, и делятся своим опытом решения этих проблем. Приходят к выводу, что согласие на обработку персональных данных может быть получено с использованием таких электронных средств коммуникации и передачи данных, как электронная почта, сервис «Yandex Forms» и подобные ему сервисы. Использование этих электронных средств коммуникации позволяет оперативно и экономно решать некоторые организационные вопросы, возникающие в образовательной практике.

Ключевые слова

персональные данные, частная жизнь, субъекты персональных данных, оператор персональных данных, согласие на обработку персональных данных, обработка персональных данных, образовательные онлайн-курсы

Для цитирования

Пятков Д. В., Сулейменова А. Р. Способы получения согласия субъекта персональных данных на их обработку в процессе организации образовательных онлайн-курсов // Юридическая наука и практика. 2023. Т. 19, № 3. С. 57–68. DOI 10.25205/2542-0410-2023-19-3-57-68

Ways to Obtain the Consent of the Subject of Personal Data for Their Processing in the Process of Organizing Educational Online Courses

D. V. Pyatkov, A. R. Suleimenova

Altai State University
Barnaul, Russian Federation

pitkov@yandex.ru

Abstract

The authors, using an example from their teaching practice, consider a special case of obtaining and processing the consent of the subject of personal data to the processing of personal data. The relationship between an educational organization and students of online advanced training courses is taken as an example. The authors show the problems they faced as organizers of educational activities and share their experience in solving these problems. They come to the conclusion that consent to the processing of personal data can be obtained using such electronic means of communication and data transmission as e-mail, the Yandex Forms service and similar services. The use of these electronic means of communication allows you to quickly and economically solve some organizational issues that arise in educational practice.

Keywords

personal data, privacy, subjects of personal data, operator of personal data, consent to the processing of personal data, processing of personal data, online educational courses

For citation

Pyatkov D. V., Suleimenova A. R. Ways to obtain the consent of the subject of personal data for their processing in the process of organizing educational online courses. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 57–68. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-57-68

Непосредственным поводом для написания статьи стала проблема, с которой столкнулись авторы в своей педагогической деятельности. На протяжении 2022 г. нами создавался и проходил апробацию массовый онлайн-курс повышения квалификации по авторскому праву. Курс создан в системе Moodle Алтайского государственного университета на базе Центра повышения квалификации. Точные сведения, касающиеся организационных и технических моментов создания курса, здесь и далее приводятся нами не случайно, поскольку во многом именно они определили характер возникших перед нами юридических проблем. После описания организационных и технических условий создания курса мы сформулируем соответствующие им юридические проблемы и попытаемся предложить их решение.

Сжатые сроки реализации проекта по созданию онлайн-курса, отсутствие опыта сбора и обработки документов, необходимых для зачисления слушателей, слабая адаптированность нашего проекта к существующей в Центре повышения квалификации практике взаимодействия со слушателями – все это заставило нас всерьез поволноваться. Особенность курса заключается в том, что он рассчитан на полностью дистанционное асинхронное обучение. Следовательно, все взаимодействие со слушателями должно происходить опосредованно, удаленно, даже на этапе принятия от них документов для зачисления на курс.

Между тем в Центр повышения квалификации до настоящего времени все организационные вопросы, связанные с зачислением слушателей, решались преимущественно традиционным образом – путем непосредственного контакта со слушателями. Как правило, занятия проводились в аудиториях, слушатели имели возможность заполнить все необходимые для зачисления документы непосредственно в Центре повышения квалификации или представить их на бумажных носителях во время первых занятий.

Очень быстро мы заметили, что теряем потенциальных слушателей именно в тот момент, когда предлагаем им оформить и представить весь необходимый пакет документов для зачисления на курс. Чтобы выполнить существующие в Центре повышения квалификации требова-

ния к оформлению документов о зачислении на курс, слушателю требовалось скачать на сайте нашего образовательного проекта пакет документов, распечатать их, заполнить и подписать соответствующие бланки, отсканировать готовые документы, переслать полученные электронные образы документов нам по электронной почте для скорейшего принятия решения о зачислении на курс, а в дальнейшем выслать подготовленный пакет документов на бумажном носителе обычной почтой. Разумеется, предполагалась и обратная связь в виде возврата слушателю одного экземпляра подписанного им договора на оказание образовательных услуг, если услуги оказывались на возмездной основе и ему такой договор требовался. Столь непростое в организационном отношении взаимодействие со слушателем вызывало вопросы особенно потому, что обучение предполагалось весьма кратковременным – 36 часов.

Стало ясно, что необходима с нашей стороны скорейшая оптимизация приема от потенциальных слушателей заявлений и зачисления их на курс. Попутно возникли вопросы к существующей практике взаимодействия со слушателями: вследствие чего она столь громоздкая, что в ней действительно необходимо и обусловлено требованиями законодательства, а что относится к разряду локальных традиций и обусловлено не самым точным пониманием законодательства и не самым удачными выбором стратегии поведения из нескольких возможных вариантов.

Комплект документов, который должен быть подготовлен в расчете на каждого слушателя включает в себя:

– заявление слушателя о зачислении на курс (иногда заявление не требовалось, можно было обойтись договором, подписание которого ясным образом выражало намерение слушателя пройти обучение, а сам договор содержал всю необходимую информацию о слушателе);

– анкету;

– договор на оказание образовательных услуг (в случае обучения на возмездной основе);

– согласие на обработку персональных данных.

На последнем документе в рамках настоящей статьи мы намерены остановиться подробнее.

Поскольку у нас как создателей и организаторов онлайн-курса отсутствовала возможность непосредственно взаимодействовать со слушателями, а вариант оформления документов на бумажном носителе с последующей пересылкой комплекта документов посредством обычной почты был для нас неприемлем по указанным выше причинам, первое решение по оптимизации приема слушателей на курс заключалось в переходе на использование скан-копий всех необходимых документов с последующейпересылкой их посредством электронной почты. Но даже этот вариант показался обременительным и для нас, и для слушателей. Отчасти коммерческая направленность проекта, обусловленная обязательствами передуниверситетом, отчасти ограниченность во времени (даже в своей некоммерческой просветительской части проект следовало завершить в сжатые сроки) – все это требовало максимально простых и оперативныхдействий по зачислению слушателей на курс. Нельзя было терять ни одного потенциального участника проекта. Но с переходом на использование скан-копий взамен оформления документов на бумажных носителях мы впервые столкнулись с опасениями со стороны коллег, ответственных за организацию работы Центра повышения квалификации. Надо заметить, что, как правило, сотрудники Центра повышения квалификации не имеют юридического образования, хорошо знают сложившуюся практику оформления документов, испытывают влияние всех бытовых предрассудков в том, что касается понимания документов, договоров, юридических процедур в целом. Забегая вперед, отметим, что нам нисколько не удалось поменять практику оформления документов и порядок зачисления на курс слушателей, проходивших обучение на возмездной основе. Коммерческий характер обучения означал, что все этапы обучения слушателя будут под пристальным вниманием ответственных сотрудников Центра повышения квалификации, тем самым обеспечивалось скрупулезное соблюдение сложившихся правил, отступить от которых не было никакой возможности, какими бы ни были наши аргументы.

К счастью, количество таких слушателей было незначительным в общей массе проходивших обучение. В том же, что касается оформления документов для зачисления на курс слушателей, обучавшихся на безвозмездной основе, здесь нам была предоставлена значительная свобода действий, который мы воспользовались. Именно этот опыт юридического решения организационных вопросов положен в основу настоящей статьи.

Итак, отказавшись от использования бумажных носителей для оформления согласия слушателя на обработку персональных данных и от услуг обычной почты, мы предпочли использовать электронный образ (скан-копию) согласия и электронную почту для получения согласия. На последнем этапе реализации проекта электронная почта была заменена электронным сервисом «Yandex Forms». Процесс сбора информации о слушателях и подготовки документов об их зачислении на курс был по нашим меркам максимально автоматизирован. В тот момент мы не решились полностью прервать связь со сложившейся практикой оформления документов и не нашли более оперативный, но допустимый, с юридической точки зрения, способ фиксации согласия слушателя на обработку персональных данных без подписания и отправки хотя бы скан-копии согласия. Поэтому сервис «Yandex Forms» был настроен таким образом, чтобы слушатель в процессе заполнения анкеты прикладывал к анкете свое согласие на обработку персональных данных. Без такого приложения отправка анкеты адресату, то есть нам, была невозможна, а следовательно, договорные отношения со слушателем сложиться не могли, он не зачислялся на курс. Здесь уместно отметить, что слушателю предлагалось скачать бланк согласия прямо на сайте, где он узнавал подробные условия предстоящего обучения и порядок оформления документов для зачисления на курс. То есть перед заполнением анкеты он мог скачать бланк согласия, подписать его, отсканировать или сфотографировать, и отправить нам полученный электронный образ согласия в качестве приложения к анкете. В самом начале проекта мы отправляли бланк согласия слушателю по электронной почте и таким же образом получали его обратно после подписания слушателем. Прогресс был очевиден, но изучение практики других участников гражданского оборота показало, что имеются механизмы получения согласия на обработку персональных данных, еще более экономные и оперативные. В дальнейшем их можно адаптировать к сервису «Yandex Forms». Но на том этапе мы в большей степени были поглощены мыслями о содержании учебного курса и не продвинулись так далеко в реформировании сложившегося механизма зачисления слушателей на курс, как могли бы на основе существующего законодательства, которое является гораздо более гибким и демократичным, нежели сложившаяся в вузовской среде бюрократическая практика. Впрочем, для точной оценки возможностей, предоставляемых законодательством, требуется обстоятельный разговор о том, что такое персональные данные среди тех многочисленных сведений, которые сообщает о себе слушатель, что такое по своей юридической природе согласие на обработку персональных данных, можно ли рассматривать его как частноправовой феномен, например как сделку, в каких случаях оно необходимо, какова степень риска для оператора персональных данных стать нарушителем закона и можно ли ее минимизировать и т. д. Переходим теперь к осуждению этих вопросов.

Согласно ст. 3 Федерального закона «О персональных данных»[1] (далее – ФЗ о персональных данных) под персональными данными следует понимать любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу. Такие сведения в большом количестве слушатели предоставляют организаторам учебных курсов, делая их операторами персональных данных: имя, дата рождения, образование, информация о документе, удостоверяющем личность и т. д.

Сбор персональных данных слушателей не является самоцелью или результатом простого любопытства работников образовательной организации. После сбора персональных данных образовательная организация совершает с полученной от слушателей информацией почти весь

[1] Рос. газета. 2006. 29 июля.

набор действий, обобщенно именуемых обработкой персональных данных: действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ о персональных данных).

Одним из условий обработки персональных данных является согласие субъекта персональных данных, в нашем случае – слушателя, зачисляемого на курс (ст. 6 ФЗ о персональных данных). Но среди случаев, когда обработка персональных данных допускается без согласия субъекта, законодатель назвал обработку персональных данных для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем. Первый вопрос, которых возникает в связи с этой нормой: обязательно ли получать согласие, если персональные данные необходимы для информирования слушателей, подготовки документов о зачислении на курс и об отчислении с курса, изготовления удостоверений о повышении квалификации и т. д.?

Строго говоря, в нашем случае можно было обойтись без получения согласия слушателя на обработку персональных данных. Чем же могла быть обусловлена практика получения таких согласий до начала нашей деятельности по созданию онлайн-курса? Ведь законодатель не проводит никаких различий между способами взаимодействия оператора и субъекта персональных данных, которые зависели бы от формы обучения. Если согласие необходимо при традиционном способе проведения занятий, т. е. непосредственно в аудитории, оно будет необходимо и при дистанционном асинхронном обучении. Верным будет и обратное утверждение. Полагаем, что две причины могли обусловить практику получения согласия слушателей в рамках договорных отношений с ними. Во-первых, фраза «обработка персональных данных необходима для исполнения договора», как содержащая условие, при котором согласие получать не нужно, не обладает той степенью определенности, которая могла бы гарантировать оператору персональных данных полную безопасность в том, что касается ответственности за нарушение законодательства о персональных данных. Необходимость обработки тех или иных персональных данных в конкретной ситуации применительно к условиям отдельно взятого договора носит оценочный характер, может вызвать более или менее обоснованные сомнения как у органов государственного контроля и надзора, так и у контрагента. Ответственность за нарушение законодательства о персональных данных носит уголовный и административный характер, что в совокупности с размером штрафных санкций заставляет оператора персональных данных задумываться о минимизации рисков привлечения к ответственности и жертвовать скоростью и простотой в оформлении отношений в пользу юридической безопасности. Во-вторых, нами было замечено, что некоторые сведения, которые по сложившейся традиции сообщают о себе слушатели, относятся к персональным данным, но совсем не нужны для исполнения договора, хотя и представляют интерес для образовательной организации. Например, в анкете, которую обычно заполняет слушатель, он указывает не только место работы, но и занимаемую должность. Вряд ли такие сведения необходимы для исполнения договора на оказание образовательных услуг, но сообщение этих сведений слушателем обязывает оператора персональных данных получать согласие слушателя на обработку персональных данных хотя бы только в этой части. Ведь один только сбор или одно только хранение подобной информации означает обработку персональных данных.

Мы приходим к выводу, что в процессе оказания образовательных услуг можно обойтись без получения согласия субъекта персональных данных на обработку этих данных, проявив максимум внимания при определении запрашиваемой у слушателя информации. Сохраняющийся при этом риск ответственности может быть минимизирован скрупулезным анализом каждого этапа взаимодействия со слушателем, отказом от сбора персональных данных, не-

обходимость которых не будет доказана в ходе внутреннего аудита договорных отношений в образовательной организации.

Но нельзя исключать, что какие-то сведения, относящиеся к разряду персональных данных, нужны образовательной организации, если не для исполнения договора, то, например, для маркетинговых исследований, для продвижения образовательного продукта и иных подобных целей. В таком случае возникает вопрос, каким образом организовать получение согласия слушателей на обработку персональных данных:

– обязательно ли оформлять письменное согласие на бумажном носителе, скрепляя его собственноручной подписью слушателя;

– можно ли заменить бумажный носитель скан-копией подписанного согласия, будет ли электронный образ согласия, представленный слушателем посредством электронной почты, иметь доказательственное значение в случае спора с надзорным органом или сами слушателем;

– является ли сервис «Yandex Forms» или иной подобный сервис адекватной заменой электронной почты, если скан-копия согласия будет признана допустимой формой согласия;

– нет ли иных более оперативных и экономных способов фиксации согласия слушателей на обработку персональных данных?

Примечательно, что законодательство о персональных данных весьма либерально решает вопрос о форме согласия. Согласно ст. 9 ФЗ о персональных данных, согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме, если иное не установлено федеральным законом. Но такая свобода выбора формы получения согласия нивелируется требованием закона к содержанию согласия: оно должно быть конкретным, предметным, информированным, сознательным и однозначным. При этом бремя доказывания факта получения согласия возлагается на оператора персональных данных. Тем не менее, стоит заметить, что даже устное согласие по общему правилу вполне допустимо.

В ФЗ о персональных данных не уточнено, что такое конкретность, предметность или однозначность согласия. Между тем законодатель весьма подробно описывает содержание согласия для тех случаев, когда оно в силу прямого указания в законе должно оформляться в письменной форме. Полагаем, что анализ требований к письменному согласию позволяет сделать общий вывод о содержании всякого согласия на обработку персональных данных. Особого внимания заслуживают требования законодателя о том, что в согласии должны быть указаны: цель обработки персональных данных; перечень персональных данных, на обработку которых дается согласие субъекта персональных данных; перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва (ст. 9 ФЗ о персональных данных). Очевидно, что доказать соблюдение всех этих предписаний оператору персональных данных будет не просто, если он не озаботится получением согласия в письменной форме, даже если она не является обязательной в конкретной ситуации. Для случаев оказания образовательных услуг при организации онлайн-курсов повышения квалификации мы не находим в законодательстве требования о письменной форме согласия.

Можно прийти к выводу, что выбор способа фиксации согласия слушателя на обработку персональных данных: на бумажном носителе, в виде скан-копии согласия, использование сервиса «Yandex Forms» и т. д. – это не вопрос о надлежащем оформлении согласия, это выбор способа доказывания факта получения согласия и его содержания. В то же время полагаем, что использование всех перечисленных способов взаимодействия со слушателем при получении согласия на обработку персональных данных вполне соответствует понятию письменной формы согласия, т. е. использование таких способов взаимодействия будет означать письменное оформление согласия даже в ситуации, когда письменная форма не является обязательной.

Согласие на обработку персональных данных можно квалифицировать как сделку. Согласно ст. 153 Гражданского кодекса Российской Федерации[2] (далее – ГК РФ) сделками признаются действия граждан и юридических лиц, направленные на установление, изменение или прекращение гражданских прав и обязанностей. Согласие на обработку персональных данных имеет все признаки сделки, поскольку является действием, направленным на возникновение юридических последствий гражданско-правового характера. Персональные данные вполне могут быть квалифицированы как объекты гражданским прав – такая их разновидность, как нематериальные блага. Например, по мнению М. Н. Малеиной, тайну персональных данных можно рассматривать в качестве разновидности тайны частной жизни, а возможность гражданина дать согласие на обработку персональных данных или отозвать согласие на обработку входит в правомочие определять судьбу персональных данных [1, с. 18]. Понятно, что при таком подходе право на обработку персональных данных вполне может рассматриваться как одно из гражданских прав, полученных оператором от субъекта персональных данных по договору с ним. Более того, само согласие на обработку персональных данных может быть составной частью договора, например договора на оказание образовательных услуг, и включаться в текст договора. Но даже если оно оформляется в виде отдельного документа, его можно квалифицировать в качестве отдельного договора между оператором и субъектом персональных данных. Мы же приходим к выводу, что даже оформляемое в виде отдельного документа согласие на обработку персональных данных является составной частью договора на оказание образовательных услуг – своего рода приложением к нему, специальным условием единого договора, оформленным отдельно от основного текста соглашения.

Следует, однако, признать, что далеко не все специалисты готовы говорить о тайне персональных данных всегда как о разновидности тайны частной жизни. Но взгляд на персональные данные как категорию, родственную тайне частной жизни, и в целом нематериальным благам, получил широкое распространение в нашем праве. Например, Р. В. Новиков пишет: «Гражданское законодательство (п. 2 ст. 2 ГК РФ) и ФЗ «О персональных данных» (ст. 2) исходят прежде всего из необходимости защиты прав граждан на неприкосновенность частной жизни, личную и семейную тайну» [2, с. 67]. Далее он весьма осторожно, но вполне определенно заявляет, что объем информации, на которую распространяется режим тайны частной, семейной и личной жизни гражданина, и информации, отнесенной законодательством к персональным данным, в целом совпадает [2, с. 68].

А. К. Жарова и В. М. Елин с опорой на ст. 24 Конституции РФ[3] отмечают, что конституционный принцип определяет право каждого человека на неприкосновенность любой информации, относящейся к прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). Авторы приходят к выводу, что конституционный принцип неприкосновенности частной жизни человека напрямую связан с персональными данными [3, с. 70]. Понятно, что если нормы ст. 24 Конституции РФ о частной жизни человека устанавливают основные принципы обработки персональных данных, то нормы гражданского законодательства о частной жизни выполняют ту же функцию.

Во всяком случае не следует забывать, что в гражданском законодательстве отсутствует исчерпывающий перечень нематериальных благ, как нет в нем и закрытого перечня объектов гражданских прав. В этой связи возможные сомнения относительно некоторых видов персональных данных – являются ли они проявлением частной жизни человека и образуют ли тайну его жизни – вполне могут быть компенсированы признанием таких персональных данных информацией особого вида, хотя и не имеющей качества тайны, но представляющей интерес для гражданского оборота, для некоторых субъектов оборота. Эта оговорка важна, поскольку

---

[2] Рос. газета. 1994. 8 дек.

[3] См.: http://publication.pravo.gov.ru/Document/View/0001202210060013 (дата обращения: 14.05.2023).

некоторые сведения, которые сообщает о себе слушатель, заполняя анкету или оформляя заявление о зачислении на курс, трудно назвать сведениями о частной жизни, еще труднее их назвать тайной. Например, сведения о месте работы и занимаемой должности вполне могут быть общедоступными. Более того, само назначение гражданина на должность может происходить публично в силу закона. Примечательно, если ГК РФ не требует получать согласие гражданина в таких случаях на сбор, хранение, распространение и использование такой информации (п. 1 ст. 152.2 ГК РФ), то ФЗ о персональных данных слишком фрагментарно решает вопрос о правовом режиме персональных данных, ставших общедоступными. Например, согласно ст. 10.1 ФЗ о персональных данных, в случае раскрытия персональных данных неопределенному кругу лиц самим субъектом персональных данных без предоставления оператору согласия, предусмотренного настоящей статьей, обязанность предоставить доказательства законности последующего распространения или иной обработки таких персональных данных лежит на каждом лице, осуществившем их распространение или иную обработку. В этой норме говорится о судьбе персональных данных, ставших общедоступными по инициативе субъекта персональных данных. Однако, в отличие от правила ст. 152.2 ГК РФ, решен вопрос о правах оператора персональных данных только применительно к распространению персональных данных, без внимания оставлены прочие способы обработки данных. Этой норме явно недостает той универсальности, которую мы видим в п. 1 ст. 152.2 ГК РФ. Впрочем, эта универсальность, возможно, предполагалась законодателем. Напротив, в ч. 1 ст. 6 ФЗ о персональных данных закреплено правило, согласно которому разрешено без согласия субъекта персональных данных осуществлять всякую обработку персональных данных, но только тех, которые подлежат опубликованию или обязательному раскрытию в соответствии с федеральным законом. Данные, ставшие общедоступными по инициативе субъекта персональных данных, здесь не упоминаются.

Почему так важен вывод о гражданско-правовой природе согласия на обработку персональных данных, отнесение его к разряду сделок? Этот вывод позволяет распространить на действия по оформлению согласия нормы о форме сделок, в частности, нормы о форме договоров. Достигается юридическая определенность в том, что касается выбора формы, субъекты получают возможность уверенно использовать все многообразие технических решений по оформлению сделок, которые приняты в гражданском обороте и легализованы законодателем.

Согласно ст. 160 ГК РФ наряду с составлением документа, выражающего содержание сделки и подписанного лицом, совершающим сделку, письменная форма сделки считается соблюденной также в случае совершения лицом сделки с помощью электронных либо иных технических средств, позволяющих воспроизвести на материальном носителе в неизменном виде содержание сделки, при этом требование о наличии подписи считается выполненным, если использован любой способ, позволяющий достоверно определить лицо, выразившее волю. Согласно ст. 434 ГК РФ договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными в соответствии с правилами абз. 2 п. 1 ст. 160 ГК РФ. Эти нормы открывают широкий простор для использования современных средств электронной связи и обмена информацией. Во всяком случае следует признать оправданным шагом в практической деятельности использование электронной почты и пересылаемых с ее помощью скан-копий согласия на обработку персональных данных. Дело даже не в том, что слушатель как субъект персональных данных ставит свою подпись на бумажном носителе, а потом присылает электронный образ документа, подтверждая таким образом свое согласие. Полагаем, что он мог бы и не подписывать экземпляр согласия на бумажном носителе и не делать его скан-копию, ограничившись пересылкой посредством электронной почты текста согласия, сопровождая пересылаемый документ пояснением, что таким образом

он выражает согласие на обработку персональных данных, для придания своему волеизъявлению однозначности и конкретности, как того требует ФЗ о персональных данных (ст. 9).

В литературе и судебной практике давно наблюдается стремление обосновать юридическое значение электронных почтовых сообщений как равных традиционным способом обмена информацией, например, на бумажных носителях. Так, например, коллектив авторов монографии «Право цифровой среды», анализируя законодательство и практику его применения, выделяют следующие виды сделок, совершаемых в электронной форме: сделки, совершаемые посредством обмена электронными документами с помощью технических средств (электронная почта, факс, смс, мессенджеры и социальные сети и др.); сделки совершаемые посредством обмена скан-копиями; сделки на электронных площадках; click-wrap-соглашения (соглашение с помощью клика мышью); browse-wrap-соглашения (совершаются путем просмотра веб-сайта); смарт-контракты [4].

Электронная почта как юридически значимый способ коммуникации при заключении договоров упоминалась в предыдущей редакции ст. 434 ГК РФ, действовавшей до 2019 г., что позволяло Верховному суду Российской Федерации дать следующее разъяснение: «При заключении договора путем обмена документами для целей признания предложения офертой не требуется наличия подписи оферента, если обстоятельства, в которых сделана оферта, позволяют достоверно установить направившее ее лицо» (п. 9 Постановления Пленума Верховного суда Российской Федерации № 49 от 25 декабря 2018 г. «О некоторых вопросах применения общих положений Гражданского кодекса Российской Федерации о заключении и толковании договора»)[4]. Последующее исключение из текста статьи слов «электронная почта» связано не с изменением позиции законодателя по поводу юридического значения электронных почтовых сообщений, а с попыткой перейти к более общим категориям, не исключающим электронную почту, а добавляющим в разряд допустимых средств коммуникации при заключении договора иных средств (наряду с электронными документами), что выразилось в словах «обмен иными данными» (ст. 434 ГК РФ) и «иные технические средства» (ст. 160 ГК РФ).

В этой связи, исследуя практику заключения договоров путем переписки в мессенджерах, Е. Панфилло ссылается на п. 13 Постановления Пленума Верховного суда Российской Федерации от 22.06.2021 № 18 «О некоторых вопросах досудебного урегулирования споров, рассматриваемых в порядке гражданского и арбитражного судопроизводства»[5] в качестве примера лояльного отношения судов не только к электронной почте как способу юридически значимой коммуникации при заключении договоров, но и к более оперативным и простым средствам связи и обмена информацией: «направление обращения с использованием информационно-телекоммуникационной сети (например, по адресу электронной почты, в социальных сетях и мессенджерах) свидетельствует о соблюдении досудебного порядка урегулирования спора исключительно в случае, если такой порядок установлен нормативным правовым актом, явно и недвусмысленно предусмотрен в договоре либо данный способ переписки является обычной сложившейся деловой практикой между сторонами и ранее обмен корреспонденцией осуществлялся в том числе таким образом» [5].

В этой связи заметим, что мы рассматриваем не конфликтную ситуацию, когда нет места формированию договоренностей о приемлемых для сторон способах коммуникации. Слушатели, заключающие договор на оказание образовательных услуг и отправляющие согласие на обработку персональных данных, знакомятся с предлагаемыми в публичной оферте способами коммуникации и, отправляя согласие на обработку персональных данных посредством электронной почты, тем самым подтверждают готовность использовать этот способ коммуникации. Поэтому разъяснение Верховного суда Российской Федерации, данное по поводу направления обращений в рамках досудебного урегулирования спора, вполне относимо и к нашей ситуа-

[4] Рос. газета. 2019. 11 янв.

[5] Рос. газета. 2021. 2 июля.

ции – использование электронной почты как способ коммуникации явно и недвусмысленно принимается участниками образовательного процесса на этапе формирования соответствующих договорных отношений.

В какой мере уместно и допустимо предположение о пригодности электронной почты, социальных сетей и мессенджеров для отправки согласия на обработку персональных данных, в такой же мере допустимо предположение о пригодности электронного сервиса «Yandex Forms» и других подобных ему сервисов. Этот сервис был использован в нашей практике как альтернативный электронной почте способ коммуникации при отправке слушателями согласия на обработку персональных данных в виде приложения к анкетам, которые они заполняли и отправляли в «Yandex Forms».

Ни ст. 160 ГК, ни ст. 434 ГК РФ, ни нормы ФЗ о персональных данных, ни разъяснения Верховного суда Российской Федерации не содержат исчерпывающего перечня электронных и иных технических средств, допустимых в процессе заключения договора. Важно соблюсти условие: избранный способ коммуникации должен позволять достоверно определить лицо, выразившее волю. Следует заметить, что сервис «Yandex Forms» использовался нами как одно из нескольких средств коммуникации со слушателями, как вспомогательное средство. Предполагалось, что с использованием сообщенной слушателем в анкете информации с ним будет заключен договор в виде отдельного документа (при платном обучении). Во всяком случае, на указанную им в анкете электронную почту высылалась информация для авторизации на электронной платформе онлайн-курса, сообщенные слушателем персональные данные использовались для подготовки приказов о зачислении на курс и об отчислении, для оформления и отправки слушателю удостоверения о повышении квалификации и т. д. При заключении договора о возмездном оказании образовательных услуг от слушателя принималась оплата услуг. Таким образом, если определенность лица, необходимая для совершения сделок, в частности для получения согласия на обработку персональных данных, может вызывать сомнения при рассмотрении отдельно взятого сервиса «Yandex Forms», то весь комплекс способов взаимодействия создает вполне достаточную определенность субъекта, оправдывая применение этого сервиса в качестве альтернативы электронной почты на первом этапе формирования договорных отношений при получении согласия слушателя на обработку персональных данных.

Согласно ст. 18 ФЗ о персональных данных, при сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации. Этому правилу соответствует норма ст. 18.1 ФЗ о персональных данных, согласно которой оператор обязан опубликовать или иным образом обеспечить неограниченный доступ к документу, определяющему его политику в отношении обработки персональных данных, к сведениям о реализуемых требованиях к защите персональных данных. Оператор, осуществляющий сбор персональных данных с использованием информационно-телекоммуникационных сетей, обязан опубликовать в соответствующей информационно-телекоммуникационной сети, в том числе на страницах принадлежащего оператору сайта в информационно-телекоммуникационной сети «Интернет», с использованием которых осуществляется сбор персональных данных, документ, определяющий его политику в отношении обработки персональных данных, и сведения о реализуемых требованиях к защите персональных данных, а также обеспечить возможность доступа к указанному документу с использованием средств соответствующей информационно-телекоммуникационной сети. Полагаем, что приведенные нормы дают большие возможности по использованию электронных сервисов не только для сбора персональных данных, но также для экономного и оперативного получения согласия субъектов персональных данных на обработку этих данных.

По нашему мнению, к этим правилам может быть адаптирована практика заключения соглашений, известных как click-wrap-соглашения, когда принятие пользователем условий дого-

вора происходит путем нажатия на кнопку «Я согласен», «I Accept» и их вариаций либо иным способом, использующим аналогичную механику [6].

В образовательной практике применение норм ст. 18 и 18.1 ФЗ о персональных данных может заключаться в отказе от оформления согласий обучающихся на обработку персональных данных в виде отдельных документов, тем более на бумажных носителях, в замене этих документов размещением на сайтах образовательных организаций общедоступных сведений под названием «политика в отношении обработки персональных данных». Важно при этом продумать и надлежащим образом организовать фиксацию факта обращения обучающегося к такой «политике» образовательной организации и согласия с ней.

Список литературы

1. **Малеина М. Н.** Право на тайну и неприкосновенность персональных данных // Журнал российского права. 2010. № 11. С. 18–28.
2. **Новиков Р. В.** Правовое регулирование защиты информации, относящейся к сфере частной жизни граждан, в гражданском законодательстве и законодательстве о персональных данных // Ex jure. 2020. № 2. С. 64–71.
3. **Жарова А. К., Елин В. М.** Источники понятий «персональные данные» и частная жизнь лица в российском праве // Вестник Академии права и управления. 2017. № 1. С. 69–78.
4. Право цифровой среды: Монография / Под. ред. Т. П. Подшивалова, Е. В. Титовой, Е. А. Громовой. М.: Проспект, 2022. 896 с.
5. **Панфилло Е.** Заключение договора путем переписки в мессенджере. URL: https://zakon.ru/blog/2022/01/25/zaklyuchenie_dogovora_putem_perepis ki_v_messendzhere issledovanie_sudebnoj_praktiki (дата обращения: 14.05.2023).
6. **Сидтиков К. Р.** Особенности click-wrap соглашений в сфере электронной коммерции: сравнительно-правовой анализ России и США // Проблемы современной экономики. 2018. № 1. С. 76–78.

References

1. **Maleina M. N.** The right to secrecy and inviolability of personal data // Journal of Russian Law. 2010. № 11. P. 18–28. (in Russ.)
2. **Novikov R. V.** Legal regulation of the protection of information related to the private life of citizens in civil legislation and legislation on personal data // Ex jure. 2020. № 2. P. 64–71. (in Russ.)
3. **Zharova A. K., Yelin V. M.** Sources of the concepts of “personal data” and private life of an individual in Russian law // Bulletin of the Academy of Law and Management. 2017. № 1. P. 69–/78. (in Russ.)
4. Law of the digital environment: Monograph / Edited by T. P. Podshivalova, E. V. Titova, E. A. Gromova. Moscow: Prospect, 2022. 896 p. (in Russ.)
5. **Panfillo E.** Conclusion of the contract by correspondence in messenger. URL: https://zakon.ru/blog/2022/01/25/zaklyuchenie_dogovora_putem_perepis ki_v_messendzhere issledovanie_sudebnoj_praktiki (accessed: 14.05.2023) (in Russ.)
6. **Sidtikov K. R.** Features of click-wrap agreements in the sphere of electronic commerce: comparative legal analysis of Russia and the USA // Problems of modern economy. 2018. № 1. P. 76–78. (in Russ.)

Информация об авторах

Дмитрий Валерьевич Пятков, кандидат юридических наук

Алия Рустемовна Сулейменова, аспирант

Information about the Author

Dmitry V. Pyatkov, Candidate of Juridical Sciences

Alia R. Suleimenova, Postgraduate Student

Статья поступила в редакцию 25.05.2023;
одобрена после рецензирования 21.06.2023; принята к публикации 31.07.2023

The article was submitted 25.05.2023;
approved after reviewing 21.06.2023; accepted for publication 31.07.2023

Научная статья

УДК 347.1
DOI 10.25205/2542-0410-2023-19-3-69-77

Проблемы защиты персональных данных в России и Китае: сравнительно-правовой анализ

Надежда Юльевна Чернусь[1,2]
Сунь Юйпэн[2]

[1]Институт философии и права СО РАН
Новосибирск, Россия

[2]Новосибирский национальный исследовательский государственный университет
Новосибирск, Россия

[1]preiudicia@yandex.ru, https://orcid.org/0000-0001-9316-524X
[2]syp19960420@163.com, https://orcid.org/0009-0001-6052-9825

Аннотация

В статье анализируется законодательство о персональных данных России и Китая, судебная практика КНР о защите персональной информации. Продемонстрировано, что законодательство России и КНР закрепляет понятие персональных данных, содержит принципы и механизм защиты персональных данных граждан, предусматривает меры ответственности за нарушение прав граждан при незаконном использовании их персональных данных. Рассмотренные примеры судебной практики КНР демонстрируют применение законодательства о персональных данных, привлечение нарушителей к гражданско-правовой, уголовной и административной ответственности. Формулируется вывод о том, что развитие интернет-технологий, технологий искусственного интеллекта, глубокого синтеза порождает множество проблем, связанных с незаконным использованием личной информации о гражданах, что требует постоянного совершенствования законодательства о защите персональных данных.

Ключевые слова

персональные данные, защита персональных данных. способы защиты персональных данных. технологии искусственного интеллекта, технологии глубокого синтеза

Для цитирования

Чернусь Н. Ю., Сунь Юйпэн. Проблемы защиты персональных данных в России и Китае: сравнительно-правовой анализ // Юридическая наука и практика. 2023. Т. 19, № 3. С. 69–77. DOI 10.25205/2542-0410-2023-19-3-69-77

Problems of Personal Data Protection in Russia and China: Comparative Legal Analysis

Nadezhda Yu. Chernus[1], Sun Yupeng[2]

[1]Federal State Budgetary Institution of Science, Institute of Philosophy and Law of the Siberian Branch of the Russian Academy of Sciences

[2]Novosibirsk National Research State University

[1]preiudicia@yandex.ru, https://orcid.org/0000-0001-9316-524X
[2]syp19960420@163.com, https://orcid.org/0009-0001-6052-9825

Abstract

The article analyzes the legislation on personal data of Russia and China, the judicial practice of the People's Republic of China on the protection of personal information. It is demonstrated that the legislation of Russia and the People's Republic of China enshrines the concept of personal data, contains the principles and mechanism of protection of personal data of citizens, provides for liability measures for violation of the rights of citizens in the illegal use of their personal data. The considered examples of judicial practice of the People's Republic of China demonstrate the application of legislation on personal data, bringing violators to civil, criminal and administrative responsibility. The conclusion is formulated that the development of Internet technologies, artificial intelligence technologies, deep synthesis generates a lot of problems related to the illegal use of personal information about citizens, which requires constant improvement of legislation on personal data protection.

Keywords

personal data; personal data protection, methods of personal data protection, artificial intelligence technologies, deep synthesis technologies

For citation

Chernus N. Yu., Sun Yupeng. Problems of personal data protection in Russia and China: Comparative legal Analysis. *Juridical Science and Practice*, 2023, vol. 19, no. 3, pp. 69–77. (in Russ.) DOI 10.25205/2542- 0410-2023-19-3-69-77

Одним из приоритетных направлений развития науки, технологий и техники в Российской Федерации является развитие информационно-телекоммуникационных систем[1]. В связи с появлением технологии искусственного интеллекта современное развитие информационных систем зависит от внедрения технологий, направленных на более совершенное функционирование любой системы, для работы которой необходимо постоянное принятие интеллектуальных, творческих решений. В целях обеспечения ускоренного развития искусственного интеллекта в Российской Федерации, проведения научных исследований в области искусственного интеллекта, повышения доступности информации и вычислительных ресурсов для пользователей, совершенствования системы подготовки кадров в этой области Президентом РФ утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года[2].

Поскольку ключевым элементом технологии искусственного интеллекта являются большие массивы данных (big data), для некоторых сфер деятельности (например, медицины) такие базы формируются из персональной информации, получение и обработка которой требует соблюдения прав обладателей этой информации. В процессе получения и обработки таких персональных данных существует угроза нарушения прав и свобод граждан, что обусловливает необходимость закрепления в законодательстве понятного и эффективного механизма защиты персональных данных граждан.

---

[1] См.: Указ Президента РФ от 7 июля 2011 г. № 899 «Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации» // Собрание законодательства РФ. 2011. № 28. Ст. 4168.

[2] Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 11 октября 2019 г.

В России в настоящее время действует Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»[3] (далее – Закон о персональных данных), который регулирует отношения, связанные с обработкой персональных данных с целью обеспечения защиты прав и свобод человека и гражданина, в том числе для защиты прав на неприкосновенность частной жизни, личной и семейной тайны. Тем не менее процесс формирования информационного общества происходит такими темпами, когда при выборе между внедрением новой технологии, использующей персональные данные, и соблюдением прав и свобод гражданина выбор делается в пользу технологий. Согласие гражданина на обработку его персональных данных приобретает формальный смысл, когда без этого согласия гражданин просто лишается возможности оперативно получить необходимую услугу. Между тем использование персональных данных приобретателями может иметь самые неблагоприятные последствия для субъекта персональных данных. Несмотря на наличие правового регулирования процессов обработки и использования персональных данных, в настоящее время до сих пор отсутствуют общие принципы обращения информации в цифровом пространстве, поскольку приоритеты между правами и свободами гражданина (защита персональных данных) и товаром (коммерческое использование персональных данных) не расставлены окончательно.

Проблема усугубляется отсутствием единого подхода к пониманию персональной информации, общего механизма ее защиты. Закон о персональных данных содержит широкое определение персональных данных, под которыми понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 Закона о персональных данных). Такое определение позволяет в различных нормативно-правовых актах использовать разные подходы к пониманию персональной информации, что позволяет придавать персональной информации отраслевую природу, когда правовое регулирование и защита персональных данных будет зависеть от характера правоотношений, в рамках которого произошло правонарушение. Например, Постановлением Правительства РФ от 30.06.2018 № 772[4] определен состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных. Данное Постановление (которое не утратило силу) было принято в соответствии с уже утратившей силу ч. 8 ст. 14.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [5] – обстоятельство, которое подтверждает отсутствие единой системы правового регулирования обработки и защиты персональной информации.

Несмотря на недостатки правового регулирования, Конституция РФ гарантирует каждому право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени. Также каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения (ст. 23 Конституции РФ). Иными словами, информация, содержащая персональные данные субъекта персональных данных, должна иметь гарантированный уровень правовой и организационно-технической защиты.

Обратимся к законодательству Китайской Народной Республики, где в августе 2019 года в целях обеспечения безопасности личной информации о несовершеннолетних были изданы «Правила защиты персональных данных детей в Сети»[6]. В сентябре 2019 года для пресече-

---

[3] Рос. газета. 2006. 29 июля.

[4] Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 03.07.2018.

[5] Рос. газета. 2006. 29 июля.

[6] Правила защиты персональных данных детей в Сети // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

ния незаконного использования приложений, собирающих личную информацию граждан, Национальная администрация киберпространства Китая обнародовала «Методы выявления незаконного сбора и использования личной информации приложениями», которые позволяют выявить незаконное использование приложений, содержащих личную информацию граждан[7]. В январе 2020 года вступил в силу Гражданский кодекс КНР (далее – ГК КНР), согласно которому персональные данные физических лиц охраняются законом (ст. 1034)[8]. Соответственно при нарушении законодательства о персональных данных граждан неправомерными действиями могут быть использованы общеправовые способы защиты, предусмотренные гражданским законодательством для защиты личных неимущественных прав. В ноябре 2021 года в Китае принят Закон КНР «О защите личной информации»[9] (далее – Закон о защите личной информации), содержащий целую систему гарантий защиты личной информации граждан. Согласно ст. 4 Закона, к личной информации относятся все виды информации, относящейся к идентифицированным или идентифицируемым физическим лицам, записанной в электронном или ином виде, за исключением анонимной информации.

Анализ Закона о защите личной информации позволяет сформулировать несколько его ключевых положений. Во-первых, Закон определяет личную информацию как такую информацию, которая не только позволяет идентифицировать определенное лицо, но и, что наиболее важно, это информация, которая также может быть использована для идентификации конкретного человека. Во-вторых, источник, в котором может содержаться личная информация, является практически любым, т. е. информация «записывается в электронном виде или иными способами». В-третьих, понятие «идентифицируемый» по отношению к обладателю персональных данных означает, что соответствующая информация не всегда может идентифицировать конкретное физическое лицо. Персональные данные могут быть объединены с информацией из другого источника или нуждаться в ином преобразовании для идентификации конкретного физического лица. Фактически лицо может быть идентифицировано при условии совершения дополнительных действий с соответствующей информацией, касающейся этого лица. В-четвертых, персональные данные принадлежат только физическим лицам, исключая юридических лиц и иные объединения. При этом физические лица могут распоряжаться своей личной информацией, в том числе посредством завещания. В-пятых, анонимизация относится к технической обработке персональных данных, при которой субъект персональных данных не может быть идентифицирован или ассоциирован, а обработанная информация не может быть восстановлена. Хотя в настоящее время полная «анонимизация» с помощью современных технологий невозможна.

С принятием в КНР Закона о защите личной информации последовало дальнейшее правовое регулирование сбора и обработки персональных данных. Так, в декабре 2021 г. Национальное сетевое информационное управление Китая приняло Положения об объеме необходимой личной информации для распространенных типов мобильных интернет-приложений[10], где «общая личная информация» граждан разделена на 39 категорий, а при ее незаконном использовании любая организация или физическое лицо, обнаружившие нарушения этих правил,

---

[7] Методы выявления незаконного сбора и использования личной информации приложениями // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[8] Гражданский кодекс Китайской Народной Республики // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[9] Закон о защите личной информации Китайской Народной Республики (от 20 августа 2021 года) // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[10] Положения об объеме необходимой личной информации для распространенных типов мобильных интернет-приложений. URL: http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm/ (дата обращения: 01.08.2023).

могут сообщить об этом в соответствующий отдел (ст. 6 Положений). Кроме того, местные законодательные органы Китая также имеют собственное законодательство о персональных данных. В частности, в 2022 г. вступило в силу Положение о данных Шэньчжэньской особой экономической зоны[11], которое является типичным примером местного законодательства Китая о персональных данных.

В настоящее время помимо Закона о защите личной информации в КНР действуют Закон об электронной подписи Китайской Народной Республики[12], Закон о безопасности данных Китайской Народной Республики[13], Закон о кибербезопасности Китайской Народной Республики[14] и другие нормативно-правовые акты, которые составляют основу законодательства о персональных данных Китая.

Множество нормативно-правовых актов, принятых в КНР, направленных на защиту личной информации граждан, позволяет сформулировать принципы правовой охраны персональных данных гражданина.

Первый принцип *информированного согласия* заключается в том, что перед обработкой персональных данных гражданина операторы обработки данных уведомляют этого гражданина указанными в законе способами и получают письменное согласие гражданина на это (либо фиксируют это согласие в форме электронных документов). В данном случае гражданин имеет право отказаться, и персональные данные гражданина не подлежат обработке. Так, согласно п. 3 ст. 24 Закона о защите личной информации, при принятии решений, оказывающих существенное влияние на права и интересы личности путем автоматизированного принятия решений, физические лица имеют право потребовать, чтобы обработчик личной информации объяснил, и имеют право отказать обработчику личной информации в принятии решений только посредством автоматизированного принятия решений. Аналогичный принцип содержится и в российском законодательстве, когда обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных (п. 1 ч. 1 ст. 6 Закона о персональных данных), возможность отказа от автоматизированной обработки его персональных данных закреплена в ч. 3 ст. 16 Закона о персональных данных.

Следующий принцип *необходимого объема обрабатываемых персональных данных* выражается в том, что объем обрабатываемых персональных данных должен соответствовать цели обработки этих персональных данных. Кроме того, оператор должен выбрать такой способ обработки персональных данных, который позволит обеспечить максимальную защиту личных прав и законных интересов субъектов персональных данных. Статья 5 Закона о персональных данных также содержит указанный принцип, включающий сразу несколько похожих положений. Во-первых, обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Во-вторых, не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, не совместимых между собой. В-третьих, обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их

[11] Портал законов Китая CJO. URL: https://ru.chinajusticeobserver.com/law/x/data-regulation-of-the-shenzhen-special-economic-zone20210629 (дата обращения: 01.08.2023).

[12] Закон об электронной подписи // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[13] Закон о безопасности данных Китайской Народной Республики от 10 июня 2021 года // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[14] Закон о кибербезопасности Китайской Народной Республики от 01 июня 2017 года // База данных национальных законов и нормативных актов. URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

обработки. Наконец, при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Оператор должен принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Следующий принцип – *отраслевого характера отношений по обработке персональных данных*. В данном случае, поскольку цели обработки персональных данных могут быть различными, начиная от автоматизированной обработки персональных данных мобильными операторами, заканчивая персонифицированным учетом, осуществляемым в отношении граждан органами публичной власти, здесь персональные данные могут быть классифицированы в зависимости от характера персональных данных на персональные данные, содержащие: личную конфиденциальную информацию, общедоступную личную информацию, биометрические данные, корпоративную информацию, финансовую информацию и др. В Российской Федерации также в различных правовых отраслях приняты положения, учитывающие особенности правоотношений, возникающих в процессе обработки персональных данных[15].

Приведенные принципы правовой охраны персональных данных обусловливают наличие целой системы мер защиты персональных данных в России и КНР. Можно выделить общие и специальные способы защиты персональных данных граждан.

Общие способы защиты гражданских прав содержатся в ст. 12 Гражданского кодекса РФ (далее – ГК РФ)[16]. Для защиты нарушенных прав, связанных с незаконной обработкой и распространением персональных данных, могут быть применены такие способы, как: восстановление положения, существовавшего до нарушения права, и пресечения действий, нарушающих право или создающих угрозу его нарушения; самозащита права; возмещение убытков; компенсация морального вреда; прекращение или изменения правоотношения; иные способы, предусмотренные законом. В ГК КНР также содержатся способы защиты гражданских прав, среди которых для защиты права на личную информацию можно выделить: пресечение действий, нарушающих закон или создающих угрозу его нарушения (ст. 997 ГК КНР); возмещение убытков (ст. 1182 ГК КНР); восстановление репутации и принесение извинения (ст. 995 ГК КНР); компенсация морального вреда (ст. 996 ГК КНР).

В качестве примера защиты прав на личную информацию можно привести дело, рассмотренное Высшим народным судом провинции Шаньдун (дело № (2020)浙0192民初10605号)[17]. Ответчик разместил два последовательных сообщений на Weibo, раскрывающих имя Чжана (истца), дату рождения, номер телефона, место жительства, место работы и другую личную информацию. После того как истец узнал об этом, он позвонил в полицию, и ответчик удалил личную информацию об истце, но продолжал размещать личную информацию против истца на Weibo. Согласно решению суда, ответчик обязан принести извинения, компенсировать моральный вред и убытки.

---

[15] См., например: глава 14 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ; глава 7 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»; ст. 84 части первой Налогового кодекса Российской Федерации от 31 июля 1998 г. № 146-ФЗ.

[16] Часть первая Гражданского кодекса Российской Федерации от 30 ноября 1994 г. № 51-ФЗ // Собрание законодательства Российской Федерации. 1994. № 32. Ст. 3301.

[17] В связи с конфиденциальной информацией данное судебное решение не было опубликовано, дело находится в ведении Высшего народного суда провинции Шаньдун. См: Шаньдунский высший народный суд 鲁司法案例[2023]071 // Официальный сайт Высшего народного суда провинции Шаньдун. URL: sdcourt.gov.cn (дата обращения: 01.08.2023).

В Уголовном кодексе КНР[18] последствиями совершения преступления, связанного с нарушением права на охрану персональных данных граждан, являются штраф и тюремное заключение (ст. 253.1 – Преступление, связанное с нарушением персональных данных граждан; ст. 286.1 – Преступление, заключающееся в отказе выполнять обязательства по управлению безопасностью информационной сети).

Согласно материалам уголовного дела, рассмотренного судом г. Ханчжоу (дело 鲁司法案例[2023]071)[19], подсудимый приобрел персональные данные граждан у других лиц через свою группу QQ (известный интернет-чат в Китае) и перевел их на свой аккаунт Baidu в облачный диск. В то же время данные неоднократно перепродавались другим лицам, и неоднократно взимались сборы на общую сумму 49 600 юаней. Согласно судебному решению, подсудимый совершил преступление, заключающееся в нарушении персональных данных граждан, и был приговорен к трем годам тюремного заключения и штрафу в размере 10 000 юаней.

Среди специальных способов защиты прав субъектов персональных данных законодательство КНР предусматривает, прежде всего, ответственность, предусмотренную главой 7 Закона о защите личной информации. Так, в соответствии со ст. 66 Закона, в случае обработки персональных данных с нарушением положений настоящего Закона или без выполнения обязательств по защите персональных данных, предусмотренных настоящим Законом, органы, отвечающие за защиту персональных данных, должны предписать нарушителю внести исправления, вынести предупреждение, конфисковать незаконные доходы, а также распорядиться о приостановке или прекращении предоставления услуг приложениями, которые неправомерно обрабатывают личную информацию; если нарушитель отказывается внести исправления, на него налагается штраф в размере не более одного миллиона юаней; и ответственные лица с прямой ответственностью и другие лица с прямой ответственностью должны быть оштрафованы на сумму не менее 10,000 100,000 юаней каждое.

В качестве примера применения специальных мер защиты прав субъектов персональных данных можно привести дело, рассмотренное судом Ханчжоу (дело № (2020) 浙0192民初10993号)[20]. Ответчик без информирования и получения согласия субъекта персональных данных зарегистрировал учетную запись с целью сбора и хранения личной информации о несовершеннолетнем лице, включая его местоположение, контактную информацию и конфиденциальные персональные данные, такие как информация о заболеваниях, изображение, голос и другие характеристики ребенка. На основании решения суда ответчик компенсировал 1,5 миллиона юаней за ущерб, причиненный правам и охраняемым законом интересам несовершеннолетнего.

Российское законодательство о персональных данных не содержит специальных способов защиты прав физических лиц, если произошло соответствующее правонарушение. Согласно ст. 24 Закона о персональных данных, лица, виновные в нарушении требований настоящего Федерального закона, несут предусмотренную законодательством Российской Федерации ответственность. Таким образом, нарушители несут гражданско-правовую, дисциплинарную, административную и уголовную ответственность в соответствии с положениями соответствующего законодательства. Так, гражданско-правовая ответственность за нарушение личных неимущественных прав предусмотрена общими положениями ГК РФ (ст. 12, 152.2 ГК РФ), административная ответственность предусмотрена Кодексом Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ[21] (ст. 13.11 предусматривает ответственность за нарушение законодательства Российской Федерации в области персональ-

---

[18] Портал законов Китая CJO. URL: https://ru.chinajusticeobserver.com/law/x/criminal-law-of-china-20171104 (дата обращения: 01.08.2023).

[19] Постановление Интернет-суда Ханчжоу от 11.03.2021 г. (2020) 浙0192民初10993号 // China Judgements Oline. URL: https://wenshu.court.gov.cn/ (дата обращения: 01.08.2023).

[20] Там же.

[21] Рос. газета. 2001. 31 дек.

ных данных). За разглашение персональных данных одного работника другим, если эти данные стали известны в связи с исполнением трудовых обязанностей, наступает ответственность в виде расторжения трудового договора по инициативе работодателя (подп. «в» п. 6 ч. 1 ст. 81 Трудового кодекса РФ от 30 декабря 2001 г. № 197-ФЗ[22]).

На основании проведенного сравнительного анализа законодательства и правоприменительной практики о персональных данных России и Китая следует прийти к выводу, что правовая система Китая в сфере защиты персональных данных содержит более эффективный механизм защиты прав граждан на личную информацию, особенно в условиях цифровизации гражданского оборота, и способствует дальнейшему развитию и совершенствованию правового регулирования отношений, возникающих в информационном (цифровом) пространстве. Развитие интернет-технологий, технологий искусственного интеллекта, глубокого синтеза порождает множество проблем, связанных с незаконным использованием личной информации о гражданах, что требует постоянного совершенствования законодательства о защите персональных данных. Уже в настоящее время широкое применение технологий глубокого синтеза требует обеспечения защиты прав граждан, чьи персональные данные могут быть незаконно использованы с целью причинения вреда этим гражданам, поскольку использование технологии глубокого синтеза позволяет, изменяя внешность и голос, вводить в заблуждение на видео и иных изображениях, нарушать права граждан на личную информацию, честь, достоинство, деловую репутацию и изображение. Технология глубокого синтеза может использоваться с целью нарушения прав граждан в киберпространстве: мошенничества, незаконных переводов денежных средств с личных счетов граждан и др. В КНР действует специальное законодательство, регулирующее использование технологии глубокого синтеза. Так, согласно ст. 23 Положения об администрировании глубокого синтеза информационных сервисов Интернета, технология глубокого синтеза относится к технологии использования глубокого обучения, виртуальной реальности и других синтетических алгоритмов для создания текста, изображений, аудио, видео, виртуальных сцен и другой сетевой информации[23]. В КНР уже начинает складываться судебная практика по делам о нарушении прав при использовании технологии глубокого синтеза. Приведем в качестве примера дело, рассмотренное судом г. Чэнду (дело № (2022) 川7101民初6349号)[24], в котором ответчик нарушил права истца, используя программное обеспечение для изменения лица на своем мобильном телефоне. Суд принял решение, согласно которому ответчик обязан немедленно удалить видео, нарушающее авторские права истца, отключить ссылку и прекратить дальнейшее нарушение прав истца на изображение.

Итак, цифровизация гражданского оборота, появление новых технологий требуют совершенствования законодательства о персональных данных. Наличие новых типов персональной информации, включая биометрические данные, появление технологий алгоритмического использования персональных данных порождают множество правовых проблем, решение которых возможно путем принятия специального законодательства о защите личных прав граждан в информационном пространстве. Специальное законодательство должно учесть изменившуюся форму общественных отношений, установить ответственность отдельных субъектов, операторов, использующих современные технологии при обработке персональных данных физических лиц.

---

[22] Рос. газета. 2001. 31 дек.

[23] Положение об администрировании глубокого синтеза информационных сервисов Интернета от 25 ноября 2022 г. // База данных национальных законов и нормативных актов URL: https://flk.npc.gov.cn/ (дата обращения: 01.08.2023).

[24] Постановление Первого железнодорожного транспортного суда Чэнду от 04.08.2022 г. (2022) 川7101民初6349号 // China Judgements Oline. URL: https://wenshu.court.gov.cn/ (дата обращения: 01.08.2023).

Информация об авторах

Надежда Юльевна Чернусь, кандидат юридических наук

Сунь Юйпэн, аспирант

Information about the authors

Nadezhda Yu. Chernus, Candidate of Law Sciences

Sun Yupeng, Postgraduate Student

Статья поступила в редакцию 20.07.2023;
одобрена после рецензирования 21.07.2023; принята к публикации 31.07.2023

The article was submitted 20.07.2023;
approved after reviewing 21.07.2023; accepted for publication 31.07.2023

Уважаемые авторы!

Журнал «Юридическая наука и практика» (ISSN 2542-0410) выпускается Институтом философии и права Новосибирского государственного университета и распространяется по подписке (подписной индекс в каталоге «Пресса России» – 11231).

В журнале публикуются материалы, соответствующие основным рубрикам: теоретико-исторические правовые науки, публично-правовые (государственно-правовые) науки. Статьи иностранных авторов, выполненные на иностранных языках, публикуются по согласованию с автором в переводе на русский язык.

Недопустимо представление в редакцию ранее опубликованных статей, а также рукописей, скомпилированных из цитат и пересказов ранее опубликованных научных работ. Автор несет ответственность за присутствие в представляемом материале любых форм заимствования. В случае обнаружения не согласующегося с законодательством об авторском праве и смежных правах заимствования материал безусловно отклоняется; дальнейшее сотрудничество журнала с автором прекращается.

Решение редакционной коллегии о принятии статьи к печати или об отклонении сообщается авторам по электронной почте.

Возвращение рукописи на доработку не означает, что статья принята к печати. Доработанный вариант необходимо прислать в редакцию вместе с ее начальной версией, рецензией ответом на замечания рецензента не позднее двух месяцев со дня его отсылки. В противном случае первоначальная дата поступления статьи при публикации не указывается.

После выхода журнала бесплатные (так называемые авторские) номера не предоставляются. Авторы самостоятельно приобретают журнал по розничной цене. Иногородним авторам возможна высылка журнала наложенным платежом по индивидуальной договоренности.

Правила оформления рукописи

Авторы представляют материалы объемом: статьи – 1 п. л., научного сообщения – 0,5 п. л., а рецензии – одной трети печатного листа на русском языке. Текст должен быть набран одним и тем же шрифтом – Times New Roman, высота шрифта – 14 пунктов, в формате Word, межстрочный интервал 1,5. Абзацный отступ – 1,25 см. Все страницы рукописи должны быть пронумерованы. Публикации, превышающие указанный объем, допускаются к рассмотрению только по согласованию с редакцией.

В тексте статьи указывается индекс УДК[25].

ФИО автора, место работы, адрес должны быть указаны на русском и английском языках.

К материалу должны прилагаться аннотация рукописи, ключевые слова, список литературы на русском и английском языках. Объем аннотации: 1000–1500 знаков с пробелами.

При несоблюдении этого требования редколлегия оставляет за собой право вернуть представленный материал автору без рассмотрения.

Библиографические ссылки: в тексте в квадратных скобках указываются номер источника, указанного в Списке литературы, номер страницы источника (для монографий и периодических изданий). Например: [12, с. 37].

В конце статьи помещается список литературы в порядке цитирования. Библиографическое описание публикации включает: фамилии и инициалы авторов (всех, независимо от их числа), полное название работы, город, название издательства или издающей организации, год

[25] См. онлайн-справочник УДК: http://teacode.com/online/udc/34/34.html

издания, том (для многотомных изданий), номер, выпуск (для периодических изданий), объем публикации (количество страниц – для монографии, первая и последняя страницы – для статьи). ***Ссылки на архивные документы оформляются в виде сноски (текст сноски располагается внизу страницы).***

В конце статьи авторы могут поместить список использованных обозначений и сокращений.

В рукописи статьи на последней странице необходимо указать следующие сведения:

- фамилия, имя, отчество (*полностью*);
- полное наименование организации – основного места работы, город, страна;
- занимаемая должность;
- ученая степень и звание (если есть);
- воинское или специальное звание (если есть);
- e-mail, ORCID (*обязательно*), SPIN и т. п. (если есть), номер мобильного, рабочего и / или домашнего телефона (*данная информация необходима для оперативного взаимодействия редколлегии с автором*).

Образец оформления рукописи

УДК 341.9

Европейское право

Иван Иванович Иванов

Новосибирский государственный университет

Новосибирск, Россия

ivan@mail.ru, https://orcid.org/xxxx-xxxx-xxxx-xxxx

Аннотация

Ключевые слова

Благодарности (если есть)

European Law

Ivan I. Ivanov

Novosibirsk State University

Novosibirsk, Russian Federation

ivan@mail.ru, https://orcid.org/xxxx-xxxx-xxxx-xxxx

Abstract

Keywords

Acknowledgements

Основной текст статьи

Список литературы / References

1. **Гладышев С. И.** Исполнительное производство в английском и российском праве: Автореф. дис. … канд. юрид. наук. М., 2001. 28 с.
2. **Gladyshev S. I.** Enforcement proceedings in the English and Russian law. Abstract of dis. ... Cand. of Sciences (Law). Moscow, 2001, 28 p. (in Russ.)

3. **Проскурин С. Г**. Эволюция права в семиотическом аспекте // Вестн. НГУ. Серия: Право. 2008. Т. 4, № 2. С. 11–18.
4. **Proskurin S. G.** Evolution of Law in semiotic aspect. *Vestnik of Novosibirsk State University. Series*: *Law*, 2008, vol. 4, no. 2, pp. 11–18. (in Russ.)

Информация об авторе / Information about the Author

Иванов Иван Иванович, кандидат юридических наук, доцент

Ivan I. Ivanov, Candidate of Sciences (Law), Associate Professor

WoS Researcher ID

Scopus Researcher ID

SPIN

Тел.: +7-111-111-11-11

Адрес редакционной коллегии

Институт философии и права
Новосибирского государственного университета
ул. Пирогова, 1, Новосибирск, 639990, Россия

Тел.: +7 (383) 266 73 79

E-mail: jurisprudence@mail.nsu.ru