


ОСОБЕННОСТИ ПРИМЕНЕНИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ В СФЕРЕ ОХРАНЫ ПЕРСОНАЛЬНЫХ ДАННЫХ


Вероника Владимировна Денисович¹, Андрей Владимирович Кудряшов², Лилианна Юрьевна Перемолотова³

¹ Казанский инновационный университет им. В. Г. Тимирязова, Казань, Россия
LtybctyejV1984@yandex.ru

 <https://orcid.org/0000-0003-3125-6570>

² Челябинский государственный университет, Челябинск, Россия
andrej.kudryashov.1975@mail.ru

³ Институт подготовки государственных и муниципальных служащих,
Академия права и управления ФСИИ, Рязань, Россия
lady.peremolotova@yandex.ru

 <https://orcid.org/0009-0005-5317-9731>

Аннотация. Наша страна особое внимание уделяет уголовно-правовой охране естественных прав человека. Каждый человек идентифицирован в обществе, нуждается в том, чтобы его уникальность была признана, уважаема и защищена. Человек остро нуждается в признании его идентичности и невозможности посягательства на те качества и свойства его личности, которые нельзя было бы повторить.

Требования основного закона страны таковы, что собирать информацию о человеке представляется в нынешних условиях рискованным и даже опасным с точки зрения не только этики поведения, но и привлечения к уголовной ответственности. Большой объем данных о человеке собирать можно только в том случае, если есть его персональное согласие и есть конкретная цель для этого, например, в рамках оперативно-розыскных мероприятий, возбужденного уголовного дела. Наша задача как правоприменителей сделать так, чтобы любое вмешательство в жизнь человека было санкционировано государством и четко определено целями и задачами закона, в том числе уголовного, и конкретного вида деятельности, в том числе правоохранительной.

Развитие этой проблемы вызывает естественную необходимость в обеспечении надежной защиты информационных ресурсов и процессов, упорядочении общественных отношений в данной сфере. Наше государство только приступает к разработке и внедрению в законодательной и исполнительной областях комплексного подхода к обеспечению защиты персональных данных посредством норм уголовного права. В этой связи особенно важно, чтобы вырабатываемый подход охватывал весь спектр проблем, а не сводился к рассмотрению лишь их технической составляющей.

Ключевые слова: персональные данные, защита персональных данных, идентификация человека, информационный ресурс, уголовно-правовой механизм защиты прав человека, кибербезопасность, информационная безопасность, киберпреступления, киберпреступность


Для цитирования: Денисович В. В., Кудряшов А. В., Перемолотова Л. Ю. Особенности применения современных цифровых технологий в сфере охраны персональных данных // Правопорядок: история, теория, практика. 2024. № 4 (43). С. 100–106. DOI: 10.47475/2311-696X-2024-43-4-100-106

Research article

PECULIARITIES OF APPLICATION OF MODERN DIGITAL TECHNOLOGIES IN THE FIELD OF PERSONAL DATA PROTECTION

Veronika V. Denisovich¹, Andrei V. Kudryashov², Lilianna Yu. Peremolotova³¹ V. G. Timiryasov Kazan Innovation University, Kazan, Russia

LtybctyejV1984@yandex.ru

 <https://orcid.org/0000-0003-3125-6570>² Chelyabinsk State University, Chelyabinsk, Russia

andrej.kudryashov.1975@mail.ru

³ Training Institute for State and Municipal Officials of the Academy of Law and Administration of the Federal Penitentiary Service, Ryazan, Russia

lady.peremolotova@yandex.ru

 <https://orcid.org/0009-0005-5317-9731>

Abstract. Our country pays special attention to the criminal-legal protection of natural human rights. Every person is identified in society, needs his uniqueness to be recognized, respected and protected. A person is in dire need of recognition of his identity and impossibility of encroachment on those qualities and properties of his personality that could not be repeated.

The requirements of the basic law of the country are such that collecting information about a person seems in the current conditions risky and even dangerous from the point of view of not only ethical behavior, but also criminal liability. A large amount of data about a person can be collected only if there is his personal consent and there is a specific purpose for this, for example, in the framework of operational-search activities, initiated criminal proceedings. Our task as law enforcers is to ensure that any interference in human life is authorized by the state and clearly defined by the goals and objectives of the law, including criminal law, and a specific type of activity, including law enforcement.

The development of this problem causes a natural necessity to ensure a reliable protection of information resources and processes, ordering of public relations in this sphere. Our state is just starting to develop and implement in the legislative and executive fields a comprehensive approach to ensure personal data protection by means of criminal law norms. In this regard, it is particularly important that the approach to be developed covers the whole range of problems, and not reduced to the consideration of their technical component only.

Keywords: personal data, personal data protection, human identification, information resource, criminal law mechanism of human rights protection, cyber security, information security, cybercrime, cybercrime

For citation: Denisovich VV, Kudryashov AV, Peremolotova LYu. Peculiarities of application of modern digital technologies in the field of personal data protection. *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2024;(4):100-106. (In Russ.) DOI: 10.47475/2311-696X-2024-43-4-100-106

Введение

За последний год в сфере защиты персональных данных произошли значительные изменения. Уголовным законодательством в данной области были утверждены и ужесточены меры ответственности за нарушения по использованию персональных данных. К новым стандартам было добавлено требование о локализации персональных данных, которое вызвало широкий резонанс в обществе. В настоящее время объем данных, которые могут быть признаны персональными в соответствии с федеральным законодательством, постоянно увеличивается, что усложняет отношения между субъектами — обладателями персональных данных и операторами. Поэтому важно проанализировать самые сложные вопросы, связанные с персональными данными, возникающие в судебной практике [4, с. 23].

В 2023 году Роскомнадзор зарегистрировал 168 утечек персональных данных, из-за которых в открытый доступ попало больше 300 млн записей о россиянах. За прошлый год суды рассмотрели 87 протоколов

Роскомнадзора, составленных по факту утечек данных, и назначили штрафы на сумму больше 4,6 млн руб. По данным ведомства, за два года сумма взысканий выросла в 23 раза: в 2021-м Роскомнадзор составил лишь четыре протокола на 200 000 руб. За 2022 год ведомство направило в суды 66 протоколов на сумму более 2,4 млн руб. Тогда в результате 140 утечек в интернет попали 600 млн записей о россиянах¹.

Необходимо сначала проанализировать, какие персональные данные нужны, как их систематизировать, какую нормативную базу исследовать, как защищать эти сведения, кого, за что и как привлекать к ответственности за незаконное распространение, а только потом приступить к сбору информации. Следует четко установить, какие данные считаются персональными, поскольку некоторые данные считаются персональными

¹ Роскомнадзор зафиксировал 168 утечек данных в 2023 году // Право.ру. URL: <https://pravo.ru/news/250809/> (дата обращения: 15.04.2024).

(как то установлено в законе), в то время как другие — нет. Например, фамилия, имя, отчество, дата рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, а также паспортные данные, адрес электронной почты четко определяются судами как персональные.

Дискуссионным остается вопрос использования электронной почты — это проблема насущная. Многим удобно общаться посредством электронного ресурса, при этом можно выбрать браузер, формат электронной почты, в некоторых случаях скрыть свои оригинальные фамилию имя и отчество. Но именно этот фактор влияет на эффективность использование электронного ресурса. Путаница также возникает, когда мы используем электронные почты личных и рабочих аккаунтов, а теперь представим, что защиты требуют несколько адресов электронной почты, т. к. у человека несколько мест работы и есть еще специальный статус. Для уголовного закона данный факт имеет существенное значение при квалификации преступления.

Когда речь идет о более сложных вопросах, таких как IP-адрес или никнейм в социальных сетях, суды имеют различные точки зрения. Одно из судебных решений представляет следующий юридический анализ IP-адреса: «идентификация пользователя сети Интернет через его персональные данные по статическому IP-адресу, назначенному оператором связи и постоянно привязанному к конечному пользовательскому оборудованию при заключении договора на предоставление услуг доступа к Интернету (при использовании статического IP-адреса все подключения пользователя всегда идентифицируются этим IP-адресом в сети связи), по своим юридическим последствиям не отличается от случаев, когда IP-адрес автоматически назначается оператором связи пользовательскому оборудованию на время подключения данного устройства (сессии) к Интернету (динамический IP-адрес)». Некоторые суды не считают IP-адрес персональными данными, в то время как другие признают (см., например, решение Арбитражного суда Челябинской области по делу № А76-29008/2015 от 11.02.2016)¹.

Существует перечень IP-адресов охраняемых законом о персональных данных. В результате принятия таких решений компании стали более осторожно относиться к обработке IP-адресов и других технических данных пользователей в своих политиках конфиденциальности. Файлам *cookie* также необходимо получать разрешение на обработку информации, которые содержат, по сути, персональные данные пользователя. (Файлы *cookie* — это текстовые файлы небольшого размера, которые устанавливаются на пользовательское устройство (телефон, компьютер), когда пользователь посещает определенный интернет-ресурс (сайт или мобильное приложение) или совершает на нем какие-то действия².)

¹ Судебные и нормативные акты РФ. URL: <https://sudact.ru/arbitral/doc/EVgK6aF1CY5A/> (дата обращения: 15.04.2024).

² Файлы *cookie* и персональные данные: терминология и основания для обработки // Право.ру. URL: <https://pravo.ru/opinion/250647/> (дата обращения: 15.04.2024).

Для этого часто используется всплывающее окно, которое информирует об использовании данной технологии и просит покинуть сайт тех пользователей, кто не согласен с этим [5, с. 25]. Однако, даже если пользователь покидает ресурс, файлы *cookie* по умолчанию остаются сохраненными на устройстве, как бы «следуя» за пользователем.

В России обсуждается вопрос о необходимости создать единую базу данные с соответствующим уровнем хранения наиболее важных IP-адресов. В материалах уголовных дела такие вопросы пока рассматриваются, но для квалификации учитываются в объективной стороне преступления и не всегда точно описываются, что может повлиять на итоговое решение суда.

Реалии сегодняшнего дня таковы, что создается совершенно уникальная категория биометрических данных человека. Современный мир достиг значительного прогресса в области применения биометрических технологий. В сфере информационных технологий биометрия относится к технологиям, которые используют уникальные физические характеристики человека для идентификации и аутентификации. Биометрические данные, их сбор, хранение, обработка, является будущностью современного мира. Посредством биометрических данных можно сформировать базу данных (по системе больших данных — Big Data), которые могут использоваться в конкретной предметной области, в том числе при создании базы данных по преступникам [2; 3].

Эти уникальные физические характеристики, известные как «биометрические данные», могут включать отпечатки пальцев, геометрию руки, сетчатку глаза, голосовые волны, подписи и черты лица. Они применяются для определения личности и упрощения процессов аутентификации. Из-за индивидуальности каждого индивида, внедрение биометрических технологий способствует повышению уровня безопасности и эффективности в различных областях, включая финансы, медицину и государственный сектор, учет осужденных и поиск преступников прошлых лет по преступлениям, совершенным достаточно давно, когда права потерпевшего не восстановлены и цель наказания в виде восстановления социальной справедливости не достигнута [1, с. 10].

Несмотря на все преимущества, использование биометрических данных не лишено опасностей, таких как возможность фальсификации, утечки и злоупотребления личной информацией, а также элементарной ошибки. Поэтому защита личных данных должна быть важнейшим аспектом при использовании биометрических технологий, учитывая непоколебимую природу таких данных [2, с. 0202].

Безопасность и конфиденциальность данных, необходимых для использования биометрических технологий, являются приоритетной задачей Российского государства. Удобство использования биометрических данных играет важную роль. Существует негативное отношение к идее создания большой централизованной базы персональных данных. Необходимо тщательно рассмотреть внедрение систем биометрической

аутентификации, чтобы избежать нарушения частной жизни граждан, а также неправомерного раскрытия конфиденциальных данных, в частности тех лиц, которые обладают специальным статусом.

В результате принятых изменений в законе, новый пароль можно легко заменить, но новую биометрическую информацию невозможно подделать. Биометрия человека не меняется в течение жизни человека, только если речь пойдет о трансплантации костного мозга человека, но это редкая и дорогостоящая операция. Во всех остальных случаях все данные, с которыми физиологически родился человек, остаются вместе с ним.

Основная часть

Особенностью оборота персональных данных многие эксперты называют его трансграничность. С развитием интернета и новых технологий, цифровизация становится неотъемлемой частью нашей жизни, что оказывает влияние на все аспекты нашего бытия. Это очевидный факт, который определяет будущее развития цифровых технологий. Несмотря на это, существует множество сложностей и противоречий, которые необходимо учитывать. Это может привести к уменьшению человеческого вмешательства и контроля в процессах, что в конечном итоге может привести к потере личной свободы и приватности. Широкое использование персональных данных приводит к увеличению числа граждан пострадавших от посягательств на эти сведения.

Специальной нормы об ответственности за нарушение Закона о персональных данных в Уголовном кодексе РФ¹ нет. Однако действия лица, нарушившего правила работы с персональными данными, могут образовать состав преступления из числа предусмотренных Уголовным кодексом РФ далее — УК РФ).

В частности, уголовная ответственность установлена:

— за незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную и семейную тайну, без его согласия (ч. 1 ст. 137 УК РФ);

— неправомерный доступ к компьютерной информации, в результате которого произошло уничтожение, блокирование, модификация (изменение) или копирование информации (ч. 1 ст. 272 УК РФ).

К уголовной ответственности могут привлечь только физическое лицо (ст. 19 УК РФ). Однако привлечение виновного физического лица к уголовной ответственности не освобождает от административной ответственности организацию (ч. 3 ст. 2.1 КоАП РФ²).

На практике часто складываются ситуации, при которых злоумышленник, движимый преступным умыслом и преследующий специальную цель, к примеру, извлечение прибыли, получает против воли владельца

доступ к цифровому ресурсу [1, с. 11]. Такие правоотношения однозначно следует отнести к категории уголовно наказуемых деяний. При этом для потерпевшего не имеет значения, получил ли он материальный ущерб, преступление будет считаться законченным с момента блокировки цифрового ресурса правонарушителем.

Таким образом, при обнаружении гражданином факта неправомерного доступа к персональным данным в цифровом пространстве, следует незамедлительно обратиться в службу технической поддержки цифрового сервиса, по возможности попытаться восстановить доступ к цифровому ресурсу, используя инструменты владельца или оператора цифрового сервиса (при их наличии). Параллельно необходимо направить заявление в правоохранительные органы по месту совершения правонарушения для установления и привлечения правонарушителя к установленному виду ответственности.

Умышленные действия, выражающиеся в незаконном сборе и распространении сведений о частной жизни человека, составляющих его личную или семейную тайну, без его согласия, влечет уголовную ответственность, предусмотренную ч. 1 ст. 137 Уголовного кодекса Российской Федерации, наказание за которое предусмотрено в виде штрафа в размере от двухсот тысяч рублей до лишения свободы на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет. Основным объектом преступного посягательства выступают общественные отношения, складывающиеся по поводу реализации конституционного принципа неприкосновенности частной жизни, личной и семейной тайны (ч. 1 ст. 23, ч. 1 ст. 24 Конституции Российской Федерации³). Факультативными объектами могут быть честь, достоинство и доброе имя человека.

Как справедливо отмечает В. И. Солдатова, «существующие меры защиты персональных данных оказываются недостаточными в современном цифровом мире, где активно применяются новые технологии» [6, с. 43], так в п. 1 ст. 3 Закона «О персональных данных»⁴ в тексте присутствует ошибка в логике, которая подразумевает, что «*информация* — это информация».

В стремлении к полному внедрению цифровых технологий и принятии множества законов законодатели и правоохранительные органы забывают об опасностях, которые могут причинить ущерб правам и интересам граждан из-за недостаточного контроля за использованием этих технологий. Несмотря на положительные стороны цифровизации, необходимо признать их негативные последствия, которые сохраняются даже при наличии государственного контроля в определенных

¹ Уголовный кодекс Российской Федерации : от 13.06.1996 № 63-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 15.04.2024).

² Кодекс Российской Федерации об административных правонарушениях : от 30.12.2001 № 195-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_34661/ (дата обращения: 15.04.2024).

³ Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года // Официальный интернет-портал правовой информации. URL: <http://pravo.gov.ru/constitution/> (дата обращения: 15.04.2024).

⁴ О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 15.04.2024).

областях (например, в процессе расследования уголовных дел и привлечения конкретного человека к уголовной ответственности). Одной из наиболее актуальных проблем является кража мобильных телефонов. Важно осознавать, что к персональным данным, например, относится номер сотового телефона, могут относиться и иные данные, и они могут быть утеряны или украдены, что может создать проблемы с безопасностью информации. Персональные данные постоянно подвергаются внешним угрозам через приложения для мобильных устройств, предоставляемые банками в России.

Процедура сбора биометрических данных является добровольной и осуществляется только с согласия клиента, однако услуга не будет предоставлена до передачи данных. Это происходит вне юрисдикции государства и контроля Банка России. Встроенная система искусственного интеллекта (роботов-ботов) не позволяет удаленно отключить данную процедуру.

При утере личных данных, таких как потеря телефона, привязанного к банковской карте, происходит большое количество правонарушений. Существует возможность незаконных действий со средствами на вашем банковском счете. В такой ситуации важно немедленно связаться с банком и следовать их инструкциям. Однако некоторые банки, использующие роботов-ботов, могут перенаправить вас в приложение, которое недоступно из-за утери телефона.

По общему мнению, средства, снятые с банковского счета в результате несанкционированного использования банковской карты до момента уведомления об этом банку, не подлежат компенсации. Таким образом, можно сделать вывод, что потребители, использующие услуги кредитных организаций, не имеют достаточной защиты, нет соответствующей нормативной базы в рамках уголовного закона.

Необходимая для обеспечения безопасности информация, персональные данные для оператора, кредитные организации и другие участники, осуществляющие обработку персональных данных, оценивают свою эффективность в этом процессе с разных позиций и точек зрения.

Анализ ст. 22.1 Закона «О персональных данных» показывает, что при обработке персональных данных необходимо принять соответствующие меры для обеспечения их безопасности, а с начала марта 2023 года эти меры вступили в силу. Благодаря приказу Роскомнадзора от 27 октября 2022 г. № 178 появились требования к оператору оценки ущерба, нанесенного гражданам при нарушении Закона «О персональных данных»¹. Оператору необходимо определить уровень возможного ущерба как высокий, средний или низкий, который должен быть отражен в документе, однако отсутствуют

конкретные требования к процессу оценки, что также свидетельствует о недостатках в системе обработки персональных данных граждан.

Согласно п. 7–12 постановления № 1119 Правительства Российской Федерации от 1 ноября 2012 года самым сложным аспектом является обеспечение безопасности электронных данных, что требует выявления конкретного типа угрозы². На основании этого представляется возможным определить необходимый уровень защиты и выбрать соответствующий набор мероприятий для обеспечения безопасности. В зависимости от выбранного уровня защиты будут предприняты определенные действия.

За нарушение законодательства о персональных данных, правил защиты, законных требований на защиту конфиденциальных сведений, а также за нарушение законодательства (подготовка необходимых документов для обеспечения законности) предусмотрены санкции. Лица, ответственные за безопасность персональных данных, могут быть привлечены к ответственности за недостаточное выполнение технических и организационных мер. Однако неясно, какие конкретные меры могут быть использованы для защиты электронных данных, что представляется проблемой в законодательстве, уголовная ответственность как таковая не предусмотрена, что представляется проблемой правоприменительной практики и требует разрешения.

На основе п. 8 ст. 19 Закона «О персональных данных» мониторинг и координация выполнения организационных и технических мероприятий по обеспечению безопасности. При обработке персональных данных в государственных базах данных персональных данных данными ограниченного доступа, проводятся ФСБ России и ФСТЭК России в соответствии с их полномочиями в сфере обеспечения безопасности и противодействия техническим разведкам и защите информации.

Как можно заметить, гл. 5 Закона «О персональных данных» посвящена государственному надзору за процессом обработки данных. Роскомнадзор, ФСБ России и ФСТЭК России названы основными контролирующими органами, однако эффективность их действий вызывает сомнения. В частности, Роскомнадзор должен улучшать защиту прав граждан, но каким образом это происходит, остается неясным. Не ясно до сих пор, какие конкретно меры данный орган предпринимает.

Итак, можно сделать вывод о том, что, несмотря на то, что цифровые технологии стали неотъемлемой частью современного правового общества в России, государство должно придавать приоритет безопасности граждан, создавая надежную систему защиты персональных данных принудительном страховании вкладов в России. Необходимо усилить нормы закона о привлечении к ответственности лиц, нарушающих правила

¹ Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»: приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 27 октября 2022 г. № 178 // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/405721227/> (дата обращения: 15.04.2024).

² Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: постановление Правительства РФ от 1 ноября 2012 г. № 1119 // СПС «Гарант». URL: <https://base.garant.ru/70252506/> (дата обращения: 15.04.2024).

обязательного страхования вкладов в банках. Необходимо предусмотреть норму, согласно которой персональные данные человека будут обеспечены персональной защитой, реальной от всевозможных посягательств.

В условиях сложной геополитической обстановки государство должно проявлять заинтересованность в защите и контроле персональных данных от нарушений на различных уровнях конфиденциальности, от несанкционированного доступа и кибератак до угроз безопасности данных; требуется усиление контрольных мер для ограничения доступа широкому кругу лиц к информации.

Более того, современная эпоха цифровизации требует признания и утверждения на уровне законодательства. Ответственность за нанесение вреда личности является неотъемлемой. При решении данных проблем в целом возможно обеспечить реальные и эффективные механизмы обеспечения безопасности и защиты персональных данных на территории РФ.

Заключение

Охрана личных данных граждан от незаконного доступа широкого круга лиц является крайне важной проблемой. Вопрос безопасности данных становится все более актуальным в условиях цифровизации всех областей общественной жизни, в том числе при предоставлении государственных и муниципальных услуг с применением информационных технологий.

Необходимо принять законодательные меры для уточнения правил передачи персональных данных граждан России за границу, их обработки иностранными органами власти и компаниями, а также для обеспечения безопасности этих данных на территории Российской Федерации и за границей.

В настоящее время вопрос обеспечения безопасности личных данных от незаконного доступа является очень актуальным. За последние годы произошло множество случаев, когда личная информация граждан была незаконно опубликована без их согласия, что указывает на неэффективность действующего законодательства в этой области.

Доступные сервисы в интернете, позволяющие получить информацию о большинстве российских граждан из различных баз данных, стали широко распространены. В них можно найти данные об адресах, наличии недвижимости, паспортных данных, номерах телефонов и других сведениях и т. п. Нарушение конституционного права на неприкосновенность личной жизни, связанное с использованием персональных данных без согласия, способствует возникновению преступлений и нарушений закона. Среди них — мошенничество, получение кредитов в обход закона, применение методов социальной инженерии.

В последнее время стало популярным новое ухищрение телефонных мошенников, которые начали активно звонить жителям России с номеров, принадлежащих странам, ранее редко используемым, таким как Иран и Сирия. Этот новый метод стал необходим из-за того, что крупные операторы связи начали блокировать звонки

с традиционных номеров. В конце октября 2022 года значительно увеличилось количество звонков от телефонных мошенников, использующих номера, начинающиеся на +9 и звучащие похоже на коды российских мобильных операторов, например +985 (похож на код Ирана), +963 (код Сирии), +903 (код Турции)¹.

Мошенники не всегда находятся на территории указанных стран, а часто используют программные способы для подмены номеров. Они сначала пытаются совершить звонок через российский номер, но операторы блокируют его, поэтому злоумышленники переключаются на иностранный номер. Операторы стараются блокировать такие звонки, но невозможно заблокировать все звонки из определенных стран, например, из Ирана (стратегического партнера России).

Закон «О защите прав потребителей» и Закон «О связи» запрещают заменять номера абонентов. Система «Антифрод»² позволит провайдерам связи проверять правильность информации о клиентах во время передачи данных.

До начала передачи персональных данных за пределы границы, оператор должен сообщить уполномоченному органу о своем намерении осуществить такую передачу и получить соответствующее разрешение. Закон определяет набор информации, содержащейся в уведомлении, включая юридическое обоснование и цель передачи и обработки персональных данных за рубежом; категории и перечень передаваемых личных данных; категории субъектов личных данных, чьи данные передаются; список иностранных государств, в которых планируется передача персональных данных через границу, а также другие подробности.

Существует опасность для жизни и безопасности граждан и их семей из-за возможности получения третьими лицами информации о недвижимости, включая адреса. Существующее законодательство не ограничивает доступ к таким данным, которые могут содержаться в Едином государственном реестре недвижимости. Поэтому информация о местонахождении объекта недвижимости и его владельце является персональными данными, требующими защиты. Законодательство поддерживает принцип открытости таких данных о владельце недвижимости.

Это является одним из требований для незаконного доступа, использования и передачи личных данных граждан.

В настоящее время вопрос обеспечения безопасности персональных данных от несанкционированного доступа является очень актуальным. За последние годы

¹ Балашова А. Телефонные мошенники перешли на использование подставных номеров из новых стран // ПБК. URL: <https://www.rbc.ru/newspaper/2022/10/28/635a27499a7947797f8063ef> (дата обращения: 15.04.2024).

² Устинова А. Роскомнадзор запустил платформу для борьбы с телефонным мошенничеством // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: <https://digital.gov.ru/ru/events/42390/> (дата обращения: 15.04.2024).

произошло множество случаев, когда личная информация граждан была незаконно разглашена, что указывает на необходимость усовершенствования действующего законодательства в этой области.

Защита личной информации граждан от несанкционированного доступа стала очень важной в современном мире, где все больше сфер жизни становятся информатизированными и используются цифровые технологии для предоставления государственных и муниципальных услуг.

Необходимо принять законодательные меры для уточнения правил передачи и обработки персональных данных граждан России за границу, а также для определения средств защиты данных как на территории России, так и за ее пределами.

В настоящее время особое беспокойство вызывает сбор личных данных для идентификации военнослужащих и сотрудников правоохранительных органов. Информация о местонахождении объектов недвижимости, включая адреса, может быть использована третьими лицами, представляя угрозу для жизни и безопасности граждан и их семей. Существующее законодательство не предусматривает ограничений на доступ к таким данным из Единого государственного реестра недвижимости. Персональные данные владельцев объектов недвижимости, содержащиеся в реестре, требуют защиты, но принцип открытости данных остается закрепленным законом.

Это является одним из требований, нарушение которого может привести к незаконному доступу, использованию и передаче личной информации граждан.

Список литературы

1. Бегишев И. Р., Кирпичников Д. В. Проблемные вопросы уголовно-правовой охраны персональных данных // Уголовная юстиция. 2020. № 15. С. 11–16.
2. Карцан И. Н. Биометрические данные: новые возможности и риски // Современные инновации, системы и технологии. 2023. № 3. 0201–0211. DOI:10.47813/2782-2818-2023-3-3-0201-0211
3. Кузнецова С. С., Мочалов А. Н., Саликов М. С. Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. С. 257–267.
4. Минбалеев А. В. Проблемы обеспечения конфиденциальности персональной информации в наследственных отношениях // Гражданское право. 2021. № 5. С. 22–29.
5. Прокопович Г. А. Теоретические аспекты и особенности института персональных данных в системе права // Администратор суда. 2024. № 3. С. 24–28. DOI: 10.18572/2072-3636-2024-3-24-28
6. Солдатова В. И. Защита персональных данных в условиях применения цифровых технологий // Lex russica. 2020. № 2. С. 19–34. DOI: 10.17803/1729-5920.2020.159.2.033-043

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

ВКЛАД АВТОРОВ

Вклад авторов равноценный.

CONTRIBUTION OF THE AUTHORS

The contribution of the authors is equivalent.

Дата поступления статьи / Received: 24.07.2024.

Дата рецензирования статьи / Revised: 14.10.2024.

Дата принятия статьи к публикации / Accepted: 05.12.2024.