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