

Неофилология

Neofilologiya = Neophilology

ISSN 2587-6953 (Print)

<http://journals.tsutmb.ru/neophilology/>

ISSN 2782-5868 (Online)

Перечень ВАК, ПИНЦ, DOAJ, Ulrich's Periodicals Directory, EBSCO, ResearchBib, CrossRef, НЭБ «eLIBRARY.RU», ЭБ «КиберЛенинка»

НАУЧНАЯ СТАТЬЯ

УДК 070

DOI 10.20310/2587-6953-2022-8-3-604-612

Персональные данные в медиасфере: специфика работы

Никита Дмитриевич МАЛЬЦЕВ

ФГБОУ ВО «Тамбовский государственный университет им. Г.Р. Державина»
392000, Российская Федерация, г. Тамбов, ул. Интернациональная, 33

✉ nw23nik@yandex.ru

Аннотация. Защита персональных данных в средствах массовой информации на современном этапе развития технологий является сложной задачей с большим количеством аспектов, которые необходимо соблюдать согласно законодательству Российской Федерации. Рассмотрены наиболее актуальные проблемы, связанные со сбором, хранением, использованием и защитой персональных данных в медиасфере. Произведена систематизация основных этапов истории развития законодательства в сфере защиты персональных данных в России и за рубежом, проведён анализ современных методов обработки, хранения и передачи персональных данных в различных странах мира. Отдельно рассмотрены законодательные акты Российской Федерации, которые применяются к определённым алгоритмам работы средств массовой информации с персональными данными. Предметно проанализирована отечественная судебная практика по случаям неправильной обработки персональных данных в средствах массовой информации. На основе результатов обобщения аналитических и статистических материалов предложены методы защиты данных при их сборе, обработке и хранении на различных этапах медиапроизводства. Полученные рекомендации могут быть использованы в практике работы редакций СМИ и в блогосфере.

Ключевые слова: персональные данные, медиасфера, технологии, защита, журналист, судебная практика

Для цитирования: Мальцев Н.Д. Персональные данные в медиасфере: специфика работы // Неофилология. 2022. Т. 8, № 3. С. 604-612. <https://doi.org/10.20310/2587-6953-2022-8-3-604-612>



Материалы статьи доступны по лицензии [Creative Commons Attribution \(«Атрибуция»\) 4.0](https://creativecommons.org/licenses/by/4.0/) Всемирная



Personal data in the media sphere: the specifics of work

Nikita D. MALTSEV

Derzhavin Tambov State University

33 Internatsionalnaya St., Tambov 392000, Russian Federation

✉ nw23nik@yandex.ru

Abstract. The protection of personal data in the media at the modern stage of technological development is a challenging task with many aspects that must be observed according to the legislation of the Russian Federation. The most pressing problems related to the collection, storage, use and protection of personal data in the media are considered. We make the systematization of the main stages in the history of the development of legislation in the field of personal data protection in Russia and abroad, an analysis was made of modern methods of processing, storing and transferring personal data in various countries of the world. The legislative acts of the Russian Federation, which apply to certain algorithms for the work of mass media with personal data, are considered separately. We analyze in detail the domestic judicial practice on cases of incorrect processing of personal data in the media. Based on the results of the generalization of analytical and statistical materials, methods for protecting data during their collection, processing and storage at various stages of media production are proposed. The recommendations received can be used in the practice of media editorial work and in the blogosphere.

Keywords: personal data, media sphere, technology, protection, journalist, jurisprudence

For citation: Maltsev N.D. Personal'nyye dannyye v mediasfere: spetsifika raboty [Personal data in the media sphere: the specifics of work]. *Neofilologiya – Neophilology*, 2022, vol. 8, no. 3, pp. 604-612. <https://doi.org/10.20310/2587-6953-2022-8-3-604-612> (In Russian, Abstr. in Engl.)



This article is licensed under a [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)



ВВЕДЕНИЕ

Сегодня цифровые технологии и технологии связи достигли такого уровня развития, что могут существенно облегчить идентификацию и поиск человека. Автоматизация технических процессов и система быстрого поиска информации существенно упрощает работу журналиста и позволяет за считанные часы собрать весь необходимый материал для статьи или видео.

Информационные технологии, которые позволяют обрабатывать большое количество информации, начали свой путь развития в начале второй половины XX века. В 1960-х гг. доступ к ним получают всё больший круг лиц, и это становится причиной опасений Совета Европы.

Первый в истории современный закон о конфиденциальности персональных данных

в ответ на опасения по поводу компьютерных достижений и конфиденциальности при обработке персональных данных был принят в 1970 г. в Гессене, Германия. Затем в 1973 г. Швеция приняла первый национальный закон о конфиденциальности под названием «Закон о данных», который криминализировал кражу данных и предоставил субъектам данных свободу доступа к своим записям.

31 декабря 1974 г. вступил в силу Закон о конфиденциальности – это федеральный закон США, устанавливающий Кодекс добросовестной информационной практики в отношении сбора, хранения, использования и распространения информации, позволяющей установить личность, федеральными агентствами¹.

¹ Защита персональных данных в США // SearchInform Information Security. URL: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh->

В 1978 г. Федеральный закон Германии о защите данных установил требование согласия на обработку персональных данных основным стандартом защиты данных. К 1979 г. многие государства-члены ЕС включили в своё законодательство законы о защите данных в качестве основных прав.

В 1983 г. в историческом деле об инвазивном характере общенациональной переписи населения Федеральный конституционный суд Германии постановил, что граждане должны иметь основное право на самоопределение в отношении своих личных данных. В постановлении установлено, что физические лица должны быть защищены от неограниченного сбора, хранения, использования и разглашения их персональных данных.

По мере развития компьютерных технологий и широкого распространения свободного обмена информацией Европейский союз (далее – ЕС) в 1995 г. принимает Директиву о защите данных, которая налагает минимальные стандарты защиты персональных данных на государства-члены и защищает права отдельных лиц в отношении перемещения персональных данных между государствами-членами ЕС².

В 2002 г. ЕС принимает Директиву о конфиденциальности и электронных коммуникациях.

В 2012 г. Европейская комиссия выпустила проект Европейского регламента по защите данных, который заменит собой Директиву ЕС о защите данных. Закон позволяет гражданам ЕС просить поисковые системы, такие как Google, удалять результаты запросов, содержащих их имя. Понятие становится известным как «право на забвение».

В странах СНГ неприкосновенность частной жизни как ценность впервые была обозначена в 1991 г. Советом РСФСР. Принятой декларацией было запрещено хранение, обработка, сбор и использование данных, если не было получено согласие субъекта данных. Именно в таком формате закон был перене-

сён в Конституцию Российской Федерации, принятую в 1993 г. В 1995 г. Нормативный правовой акт отнёс персональные данные к конфиденциальной информации [1].

Исследователь Л.В. Криволапова в своей работе отмечает, что в гражданском законодательстве неприкосновенность личной жизни гражданина обеспечиваются предоставлением ему личных неимущественных прав, которые позволяют охранять от постороннего вмешательства его поведение в индивидуальной жизнедеятельности [2]. Это означает, что не любая информация, найденная в сети Интернет, может быть законно использована в публикации. На территории Российской Федерации правоотношения в области персональных данных (далее – ПД) регулируются Федеральным законом № 152-ФЗ «О персональных данных». В судебной базе существует множество прецедентов случайного или умышленного распространения ПД журналистами и редакциями, а в сети Интернет всё чаще поднимаются вопросы конфиденциальности и безопасности данных.

ПОСТАНОВКА ЗАДАЧИ

В связи с изложенным необходимо произвести анализ судебных прецедентов по делам о разглашении персональных данных, рассмотреть, как производится защита данных на государственном уровне, произвести исследование зарубежной практики в области защиты ПД. Выявление тех или иных признаков нарушения обработки персональных данных журналистом и их последующая систематизация позволит существенно снизить возможность появления новых прецедентов, что обуславливает актуальность задачи исследования работы с персональными данными в медиасфере.

Основополагающим методом исследования является метод анализа, включающий в себя дедукцию и аналогию. Также в работе применены статистические и классифицирующие методы для более детального исследования проблемы.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

1. Отечественная практика работы с персональными данными в медиасфере.

dannyykh/realizaciya-zashchity-personalnyh-dannyh/mezhdunarodnaya-sistema-zashchity-personalnyh-dannyh/v-ssha/ (дата обращения: 12.05.2022).

² ePrivacy Regulation and its shadow! What to expect // Digital Guide IONOS. 2020. 9 of February. URL: <https://www.ionos.com/digitalguide/websites/digital-law/eprivacy-regulation-about-the-eus-privacy-policy> (accessed: 10.05.2022).

Согласно Федеральному Закону № 152-ФЗ, персональные данные – это любая информация, относящаяся к прямо или косвенно к определённому или определяемому физическому лицу (субъекту персональных данных) (пункт 1 статьи 3 № 152-ФЗ «О персональных данных»).

В законе указывается, что к персональным данным относятся:

- фамилия, имя, отчество;
- пол;
- возраст;
- дата и место рождения;
- образование и квалификация;
- профессиональная подготовка и сведения о повышении квалификации;
- гражданство;
- место жительства;
- номер телефона;
- семейное положение, наличие детей, родственные связи;
- изображение человека (фотография и видеозапись), которое позволяет установить его личность.

Однако с фото- и видеоматериалами, на которых изображены люди, есть исключения. Объектом персональных данных изображение будет являться лишь в том случае, если есть указание на имя и фамилию и/или должность или другие особенности, которые позволят идентифицировать человека.

В федеральном законе выделено несколько категорий персональных данных:

- специальные категории персональных данных – касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъекта (пункт 1 статьи 10 № 152-ФЗ «О персональных данных»);

- биометрические персональные данные – физиологические и биологические особенности человека, на основании которых можно установить его личность (пункт 1 статьи 11 № 152-ФЗ «О персональных данных»).

Стоит отметить, что в законе прямо не указан точный перечень биометрических персональных данных. В связи с чем Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций выпустила разъяснение, где

был дан примерный список физиологических данных, который можно отнести к биометрическим персональным данным, а именно: дактилоскопические данные, радужная оболочка глаз, анализы ДНК, рост, вес и др. Также фото- или видеоматериалы относятся к биометрическим персональным данным, если они позволяют идентифицировать личность человека.

Тема персональных данных в современной России очень актуальна, так как многие системы обработки, хранения информации активно цифровизируются, повышается количество обрабатываемых данных. Для СМИ данная тематика также является актуальной, поскольку журналисты работают не только с людьми, но и большим потоком информации, в котором могут скрываться как свободные, так и закрытые данные, а значит, каждый работник СМИ должен уметь разделять на категории получаемую извне информацию и понимать, какие санкции могут быть наложены за нарушения при работе с данными.

В судебной практике есть множество прецедентов, когда журналисты, готовя сюжет, совершали ошибку и публиковали материал, в котором содержались персональные данные. За последние несколько лет можно выделить несколько показательных случаев.

В 2018 г. в Воронежской области рассматривалось дело, в котором фигурировал интернет-портал, опубликовавший новость о противоправных действиях в отношении несовершеннолетнего. В публикации использовалась фотография подростка без согласия родителей/ребёнка, что запрещено законодательством РФ. Интернет-портал имел свидетельство о регистрации как СМИ и потому был привлечён к административной ответственности³.

В 2014 г. в Республике Саха было рассмотрено дело о газетной публикации, в которой указывались персональные данные заявителя без его согласия. Мировой судья вынес постановление, согласно которому

³ Обзор практики разрешения судами споров, связанных с административным правонарушением в отношении Лебедева П.А. // База данных Российской судебной практики по информационному праву. 2018. 18 янв. URL: <https://media-pravo.info/case/1763-2> (дата обращения: 10.05.2022).

автор статьи был признан виновным, и ему был назначен штраф⁴.

Конечно, подобные случаи возникают, но зачастую дела возбуждаются вследствие освещения журналистами общественно-значимых тем.

В 2013 г. в Свердловской области рассматривалось дело о публикации статьи в газете без получения согласия субъекта ПД. В материале содержались следующие сведения о гражданине: имя, фамилия, год рождения, образование, город проживания, рабочая должность, сведения об отсутствии судимости, обстоятельства преступления. Автор статьи пояснил, что никакого ущерба чести и достоинства гражданина указанием его ПД не причинено, размещение данной статьи было в целях предупреждения и профилактики подобных преступлений. Суд вынес постановление и подверг автора статьи наказанию в виде предупреждения⁵.

В 2008 г. в Курской области в районной газете была опубликована статья об изъятии детей из неблагополучной семьи и взятии их под контроль государства. В публикации были разглашены персональные данные детей, и суд пришёл к выводу о том, что журналист совершил административное правонарушение. Однако от наказания автор статьи был освобождён, так как публикация была посвящена общественно-важной теме.

Как можно заметить, иногда журналисты вынуждены публиковать материалы с персональными данными без получения согласия, если статья носит разоблачительный характер.

Законом предусмотрены отдельные случаи, когда можно публиковать персональные данные без согласия владельца. К таким случаям относятся:

- распространение общественно-важной информации;

- если журналист осуществляет свою профессиональную деятельность; если ПД общедоступны (государственные реестры и т. д.);

- если ПД содержатся в документах, которые подлежат официальному опубликованию.

Однако в законе также указано, что даже в этих случаях разглашение персональных данных не должно нарушать права субъекта ПД.

Все зарегистрированные СМИ страны обязаны соблюдать законы Российской Федерации. Вследствие чего усложняется фильтрация, проверка и обработка данных при подготовке материала [3].

Журналист обязан:

- соблюдать устав редакции, с которой он состоит в трудовых отношениях;

- получать согласие (за исключением случаев, когда это необходимо для защиты общественных интересов) на распространение в средстве массовой информации сведений о личной жизни гражданина от самого гражданина или его законных представителей;

- ставить в известность главного редактора о возможных исках и предъявлении иных предусмотренных законом требований в связи с распространением подготовленного им сообщения или материала.

Любые действия, совершаемые с ПД, являются их обработкой, которая осуществляется только с разрешения субъекта персональных данных. Данное требование имеет и исключение, если информация заимствуется из открытых источников. Таковыми могут являться справочники или адресные книги (пункт 1 статьи 8 № 152-ФЗ «О персональных данных»).

Таким образом, чтобы журналисту выпустить материал и не нарушить закон, необходимо получить согласие на обработку персональных данных или же соблюсти условия свободного использования персональных данных всех субъектов, чьи права затрагивает данный материал. Но существует вероятность столкнуться с кражей персональных данных или их искажением на момент написания или публикации материала, так как персональные данные становятся всё более востребованными у злоумышленников.

Сегодня существуют несколько способов защиты персональных данных:

⁴ Обзор практики разрешения судами споров, связанных с заявлением Управления Роскомнадзора по Республике Саха (Якутия) // База данных Российской судебной практики по информационному праву. 2014. 18 июля. URL: <https://media-pravo.info/case/1083-2> (дата обращения: 10.05.2022).

⁵ Обзор практики разрешения судами споров, связанных с административным правонарушением, предусмотренного ст. 13.11, в отношении ООО Медиа-Группа «Городские Вести» // База данных Российской судебной практики по информационному праву. 2013. 1 февр. URL: <https://media-pravo.info/case/902-2> (дата обращения: 10.05.2022).

- использование антивирусного программного обеспечения на персональном компьютере, где производится обработка, хранение и передача персональных данных;

- аккуратное обращение с метаданными (метаданные – это данные о документе, электронном файле или другом носителе информации, которые содержат их состав, содержание, информацию о геолокации их создания, качестве, формате, объёме и др.), фото-, видео- и текстовыми материалами при их загрузке в сеть Интернет, не хранить обрабатываемые данные в облачных сервисах.

Согласно отчету Info Watch за 2020 г., в России 53 % утечек персональных данных приходится на облачные сервисы и сеть Интернет. Второе и третье место занимают утечки по электронной почте и бумажной документации⁶. По данным опроса ВЦИОМ, в 2021 г. более трети россиян (37 %) не знали, для чего и как могут использоваться их персональные данные, и только 15 % опрошенных отметили, что точно знают, зачем производится сбор и обработка их персональных данных⁷. В 2021 г. Роскомнадзор обработал более 38 тысяч жалоб граждан на неправомерную обработку персональных данных. Наибольшее количество жалоб поступало на владельцев интернет-ресурсов, в том числе на владельцев интернет-сайтов⁸.

Зачастую злоумышленники используют полезные программы, как оболочку для своих вирусов. Так, скачав текстовый файл и открыв его, можно активировать вирусное ПО, которое попытается украсть персональные данные пользователя или данные, хранящиеся на жёстком диске компьютера. Та-

кие программы называют стиллерами [4]. Для предотвращения подобных атак необходимо использовать антивирусное ПО, которое будет сканировать скачиваемые файлы и помещать их в карантин, если это потребуется.

Не стоит забывать и про метаданные, которые собирают и хранят все устройства и используются журналистами, операторами и редакторами на производстве [5]. Например, если для редактирования текста используется MS Office, необходимо соблюдать осторожность с тем, какие данные попадут в метаданные файла. MS Office хранит в себе количество печатей файла, учётную запись пользователя, который создал файл, дату и время создания, а также изменения файла. Если же в редакции возникнет конфликтная ситуация, метаданные могут быть использованы для её разрешения.

Облачные сервисы – ненадёжное средство хранения или передачи информации. Частые взломы и хищения файлов с хранилищ могут нанести большой ущерб как редакции, так и физическим лицам, персональные данные которых были утрачены. Если и использовать общее хранилище для такого типа файлов, то только без подключения в сеть Интернет.

Блогеры также являются операторами персональных данных, если на сайте блога используется регистрация с указанием имени, фамилии и номера телефона или авторизация через социальные сети. Использование данных пользователей без их согласия неправомерно.

П.С. Швыряев в своей статье отмечает, что в 2020 г. наибольшее число утечек было со стороны внутренних нарушителей – сотрудников организаций [6].

По данным Global Cybersecurity Index, в 2020 г. Россия заняла 8 место по уровню кибербезопасности в мире. Уровень защищённости страны равен 98,6 % и оценивается по пяти параметрам: техническая, организационная подготовленность, юридическая, готовность к сотрудничеству, развитие образовательного и исследовательского потенциала страны. Первую строку таблицы занимает США с показателем в 100 %⁹. Таким обра-

⁶ Утечки информации ограниченного доступа: отчёт за 9 месяцев 2020 г. // Экспертно-аналитический центр InfoWatch. 2020. URL: https://d-russia.ru/wp-content/uploads/2020/12/infowatch_2020_9_monts_data_1_eak.pdf (дата обращения: 11.05.2022).

⁷ Сохранность персональных данных. Аналитический обзор // ВЦИОМ. Ассоциация больших данных. 2021. 07 сент. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/sokhrannost-personalnykh-dannykh> (дата обращения: 10.05.2022).

⁸ Подведены итоги работы Роскомнадзора в 2021 году по защите прав и интересов граждан в сфере персональных данных // Федеральная Служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). 2022. 2 февр. URL: <https://rkn.gov.ru/news/rsoc/news74048.htm?print=1> (дата обращения: 10.05.2022).

⁹ Global Cybersecurity Index 2020. Measuring commitment to cybersecurity // Global Cybersecurity Index.

зом, из собранной статистики можно сделать вывод, что наиболее опасным местом хранения, обработки и передачи информации является сеть Интернет, а также стоит обращать внимание на сотрудников редакции, которые занимаются персональными данными.

В случае обработки персональных данных без согласия субъекта персональных данных либо с нарушением требований к составу сведений, включаемых в обработку, гражданам грозит штраф от 3 тысяч рублей до 5 тысяч рублей, должностным лицам от 10 тысяч рублей до 20 тысяч рублей, юридическим лицам от 15 тысяч рублей до 75 тысяч рублей.

За невыполнение оператором в установленные сроки требования субъекта персональных данных или его представителя либо Роскомнадзора об уточнении персональных данных, их блокировании или уничтожении (если данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки) налагается штраф на граждан от 700 рублей до 2 тысяч рублей, на должностных лиц от 4 тысяч рублей до 10 тысяч рублей, на юридических лиц от 25 тысяч рублей до 50 тысяч рублей.

За незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или СМИ налагается штраф до 200 тысяч рублей либо обязательные работы на срок до 360 часов¹⁰.

2. Зарубежная практика работы с персональными данными в медиасфере. В 2016 г. Европейский союз принял Общий регламент по защите данных (GDPR). Данный закон о конфиденциальности и безопасности является одним из строжайших в мире. Несмотря на то, что он был разработан и принят Европейским союзом, он налагает

обязательства на все организации, если они собирают данные, связанные с людьми из ЕС. Постановление вступило в силу 25 мая 2018 г. GDPR налагает суровые штрафы на тех, кто нарушает его стандарты конфиденциальности и безопасности. Штрафы достигают десятков миллионов евро.

Согласно этому документу, оператор персональных данных обязан производить обработку в соответствии с принципами защиты и подотчётности: законность, справедливость и прозрачность.

В законе перечислены ситуации, когда обработка персональных данных является законной:

- субъект данных дал конкретное, недвусмысленное согласие на обработку данных;
- обработка необходима для выполнения или подготовки к заключению договора, стороной которого является субъект данных;
- необходимо обработать ПД, чтобы выполнить юридические обязательства;
- необходимо обработать данные, чтобы спасти чью-то жизнь;
- обработка необходима для выполнения задачи в общественных интересах или для выполнения какой-либо официальной функции;
- присутствует законный интерес к обработке чьих-либо персональных данных.

В GDPR персональными данными является любая информация, которая относится к физическому лицу, и оно может быть прямо или косвенно идентифицировано. Имена и адреса электронной почты, очевидно, являются личными данными. Информация о местонахождении, этническая принадлежность, пол, биометрические данные, религиозные убеждения, веб-куки и политические взгляды также могут быть персональными данными. Псевдонимные данные также могут подпадать под это определение, если по ним относительно легко кого-то идентифицировать.

В 2017 г. Европейской комиссией опубликован первый проект реформы ePrivacy. Основной целью реформы является повышение уровня личной защищённости граждан Европейского союза при использовании цифровых каналов связи. Изменения директивы касаются политики обработки персональных данных крупными интернет-компаниями. Важным дополнением в дирек-

URL: <https://nonews.co/wp-content/uploads/2021/09/GCI-2020.pdf> (accessed: 12.05.2022).

¹⁰ Commission proposes high level of privacy rules for all electronic communications and updates data protection rules for EU institutions // European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_16 (accessed: 12.05.2022).

тиве является ограничение по сбору и обработке cookie-файлов. Администраторы сайтов смогут использовать данные пользователей только после явного согласия на их обработку. Также если пользователь не согласен на передачу своих данных администратору, он вправе получить предоставляемый контент в полном объеме. Для реализации подобной технологии может использоваться настройка браузера по умолчанию [7].

Возможным последствием принятия реформы может стать ситуация, когда владельцы медиа-порталов и СМИ лишатся доли заработка, так как файлы cookie используются для предоставления пользователю предпочтительной для него рекламы и контента. Предоставление таргетированной рекламы будет возможно только после явного согласия пользователя [7].

ВЫВОДЫ

Таким образом, сегодня персональные данные являются важным инструментом не только для журналистов, компаний, но и для любого человека, и с каждым годом становятся всё более важным звеном правовых отношений между средствами массовой информации и гражданами Российской Федерации. Особое внимание как обычным гражданам, так и журналистам стоит уделять правильному сбору, обработке, хранению и за-

щите персональных данных, ведь данная сфера регулируется в Российской Федерации на законодательном уровне, и её нарушение влечёт за собой ответственность. Цифровизация и всё больший переход изданий в сеть Интернет влечёт за собой новые угрозы для владельцев интернет-порталов и интернет-СМИ, так как персональные данные приобретают всё большую ценность.

Научная новизна заключается в систематизации имеющихся знаний, а также в исследовании отечественной и зарубежной практики по защите персональных данных, что позволяет выявить правила безопасного обращения с персональными данными в медиасфере.

Значение проведённого исследования на практике состоит в конкретизации и систематизации неоднозначных моментов при работе с персональными данными в СМИ, а также в анализе методов защиты персональных данных при обработке при производстве контента.

Работа рассматривает только один из аспектов проблемы. В дальнейшем могло бы быть произведено более глубокое исследование процесса сбора и обработки биометрических персональных данных при помощи технических средств на основном этапе производства телесюжета. Данная проблема является наиболее актуальной, так как затрагивает большую часть современной медиасферы.

Список источников

1. *Волеводз А.Г.* Защита персональных данных в Европейском союзе: правовое регулирование и порядок взаимодействия с третьими странами // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 303-312.
2. *Кривопалова Л.В.* Защита персональных данных // Право и государство: теория и практика. 2020. № 6 (186). С. 88-91.
3. *Донских А.Г.* Актуальные проблемы использования персональных данных в деятельности СМИ // Вестник НГУ. Серия: История, Филология. 2021. Т. 20. № 6: Журналистика. С. 145-155. <https://doi.org/10.25205/1818-7919-2021-20-6-145-155>
4. *Останний Д.О.* Стиллер «(s)AINT» и защита от него // Юный учёный. 2019. № 1 (21). С. 7-13. URL: <https://moluch.ru/young/archive/21/1358/> (дата обращения: 25.04.2022).
5. *Kuksov I.* Как невидимые данные электронных документов приводят к реальным проблемам // Kaspersky.ru. 2017. 9 марта. URL: <https://www.kaspersky.ru/blog/office-documents-metadata/14277/> (дата обращения: 10.05.2022).
6. *Швыряев П.С.* Утечки конфиденциальных данных: главный враг внутри // Государственное управление. Электронный вестник. 2022. № 91. С. 226-241.
7. *Гуде С.В. Арбузов П.В., Карника А.Г.* Защита персональных данных в Российской Федерации: исторический аспект и современное состояние // Юрист-Правовед. 2015. № 2 (69). С. 93-97.

References

1. Volevodz A.G. Zashchita personal'nykh dannykh v Evropeyskom soyuze: pravovoye regulirovaniye i poriyadok vzaimodeystviya s tret'imimi stranami [Protection of personal data in the European union: legal regulation and procedure for cooperation with third countries]. *Biblioteka kriminalista. Nauchnyy zhurnal. – Criminalist's Library. Scientific Journal*, 2018, no. 3 (38), pp. 303-312. (In Russian).
2. Krivopalova L.V. Zashchita personal'nykh dannykh [Protection of personal data]. *Pravo i gosudarstvo: teoriya i praktika – Law and State: The Theory and Practice*, 2020, no. 6 (186), pp. 88-91. (In Russian).
3. Donskih A.G. Aktual'nyye problemy ispol'zovaniya personal'nykh dannykh v deyatelnosti SMI [Current problems of using personal data in media activities]. *Vestnik NGU. Seriya: Istoriya, Filologiya – Bulletin of the Novosibirsk State University. Series: History, Philology*, 2021, vol. 20, no. 6: Journalism, pp. 145-155. <https://doi.org/10.25205/1818-7919-2021-20-6-145-155> (In Russian).
4. Ostanniy D.O. Stiller «(s)AINT» i zashchita ot nego [Stiller “(s)AINT” and protection against it]. *Yunnyy uchenyy – Young Scientist*, 2019, no. 1 (21), pp. 7-13. (In Russian). Available at: <https://moluch.ru/young/archive/21/1358/> (accessed 25.04.2022).
5. Kuksov I. Kak nevidimyye dannyye elektronnykh dokumentov privodyat k real'nyim problemam [How invisible data of electronic documents lead to real problems]. *Kaspersky.ru*, 2017, 9 March. (In Russian). Available at: <https://www.kaspersky.ru/blog/office-documents-metadata/14277/> (accessed 10.05.2022).
6. Shvyryaev P.C. Utechki konfidentsial'nykh dannykh: glavnyy vrug vnutri [Data breaches: the main enemy within]. *Gosudarstvennoye upravleniye. Elektronnyy vestnik – E-Journal Public Administration*, 2022, no. 91, pp. 226-241. (In Russian).
7. Gude S.V., Arbuzov P.V., Karpika A.G. Zashchita personal'nykh dannykh v Rossiyskoy Federatsii: istoricheskiy aspekt i sovremennoye sostoyaniye [Personal data protection in the Russian Federation: historical aspects and current condition]. *Yurist'-Pravoved* [Lawyer-Legislator], 2015, no. 2(69), pp. 93-97. (In Russian).

Информация об авторе

Мальцев Никита Дмитриевич, аспирант, кафедра журналистики, рекламы и связей с общественностью, Тамбовский государственный университет им. Г.Р. Державина, г. Тамбов, Российская Федерация, ORCID: [0000-0003-0628-2486](https://orcid.org/0000-0003-0628-2486), nw23nik@yandex.ru

Вклад в статью: идея, сбор данных, написание текста статьи.

Поступила в редакцию 05.07.2022
Одобрена после рецензирования 08.09.2022
Принята к публикации 16.09.2022

Information about the author

Nikita D. Maltsev, Post-Graduate Student, Journalism, Advertising and Public Relations Department, Derzhavin Tambov State University, Tambov, Russian Federation, ORCID: [0000-0003-0628-2486](https://orcid.org/0000-0003-0628-2486), nw23nik@yandex.ru

Contribution: idea, data acquisition, manuscript text drafting.

The article was submitted 05.07.2022
Approved after reviewing 08.09.2022
Accepted for publication 16.09.2022