DOI 10.37882/2223-2974.2025.08.14

ПОДХОД К ПОНИМАНИЮ СОДЕРЖАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ КАК ОБЪЕКТА УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

APPROACH TO UNDERSTANDING THE CONTENT OF PERSONAL DATA AS AN OBJECT OF CRIMINAL LAW PROTECTION

V. Pekareva

Summary. In modern theoretical and practical jurisprudence, the question of achieving a balance between ensuring the security of personal data and the use of personal information in the flow of various information and manipulations with them remains difficult to answer unambiguously. In order to counteract illegal acts committed using information and communication technologies and to prevent them using general scientific and private scientific methods of cognition of reality, a study of the concept of personal data, as well as related key issues, has been conducted in scientific work. The author's representation of the essence of the definitive characteristics of the specified concept and its structural elements falling under the protection of criminal legislation is proposed.

Keywords: unauthorised access, personal data, biometric data, computer information, criminal law, identification, personal data leakage.

Пекарева Виктория Владимировна
Академия права и управления ФСИН России, г. Рязань
viktoria.pekareva@yandex.ru

Аннотация. В современной теоретической и практической юриспруденции пока остаётся сложным для однозначного ответа вопрос достижения баланса между обеспечением безопасности персональных данных и использованием личной информации в потоке различных сведений и манипуляций с ними. В целях противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, и их профилактики общенаучными и частнонаучными методами познания действительности в научной работе проведено исследование понятия персональных данных, а также связанных с ним ключевых проблем. Предлагается авторское представление сущности дефинитивных характеристик указанного понятия и его структурных элементов, попадающих под охрану уголовного законодательства.

Ключевые слова: неправомерный доступ, персональные данные, биометрические данные, компьютерная информация, уголовный закон, идентификация, утечка персональных данных.

Защита и правильное использование такой правовой и технической категории, как персональные данные, в совокупности требует единства в вопросах координации и контроля реализации правовых и организационных мер, что позволяет предотвратить возможные нарушения прав граждан, завладев их личной информацией. С развитием цифровых технологий любые сведения, связанные непосредственно с человеком, становятся персональными. Вся эта информация быстро может быть доступной в Интернете и сохраниться в различных базах данных, которые можно продавать и использовать для идентификации личности. Например, достаточно несколько точек постоянной геолокации, чтобы «выйти на человека». Подобное стало возможным по причине того, что некоторая информация, которая изначально считалась неидентифицируемой, может быть преобразована теперь в личную информацию при определенных условиях, а косвенно идентифицируемая информация может быть преобразована в напрямую идентифицируемую.

Совершенно справедливым можно считать обозначение набирающей обороты проблему того, что с каждым новшеством в области технологий нарастает вероятность неблагоприятного исхода при взаимодействии тех, кто подвержен опасности в большей степени в информационном пространстве по различным субъективным и объективным причинам, и другими лицами, которые извлекают выгоду от указанных субъектов ранее.

Изучение вопросов обеспечения информационной безопасности, в частности защиты персональных данных, от негативных вмешательств обусловлено особенно актуальными факторами:

1) Введение 30 ноября 2024 года нового состава преступления в главу 28 УК РФ, согласно Федеральному закону от 30.11.2024 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». Этот закон устанавливает уголовную ответственность за использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные, полученной неправомерным доступом к средствам ее обработки или хранения, а также за создание и обеспечение функционирования информационных ресурсов для незаконного хранения и распространения таких данных;
2) Количественные показатели негативных проявлений совершения противоправных деяний с использованием информационно-коммуникацион-

ных технологий, содержание которых оставляет желать лучшего;

3) Принятие Правительством Российской Федерации распоряжением от 30 декабря 2024 года № 4154-р концепции государственной системы противодействия противоправным деяниям, совершаемым с использованием информационно-коммуникационных технологий, в которой определены стратегические задачи, направления и подходы к обеспечению информационной безопасности, включая обязательство создания надежного барьера против преступлений, связанных с неправомерным доступом к компьютерной информации и утечками конфиденциальных данных, что может нанести ущерб как отдельным лицам, так и организациям, в том числе в оборонно-промышленном комплексе и смежных отраслях;
4) Цифровая трансформация способствует модернизации механизма совершения преступлений и стремлению прибегать к более изощренным методам среди злоумышленников.

Целью является установить какие именно типы персональных данных обозначены при незаконных альтернативных действиях в виде использования, сбора, передачи, хранения и распространения определены уголовным законом; осуществить интерпретационный процесс частей персональных данных как целого для характеристики их особенностей, выявления причин совершения преступлений с личной информацией граждан, неурегулированных моментов и трудностей обеспечения защиты. Анализ поставленного вопроса помогает осознать уязвимости устройств и систем, а также понять, какие действия и меры предосторожности могут быть предприняты для безопасности персональных данных как на индивидуальном уровне, так и на управленческом, государственном.

Ограничение доступа к популярным интернет-сервисам и социальным сетям в России в период с 2022 по 2024 гг., таких как LinkedIn, YouTube, Rutracker, Facebook, Instagram, TikTok и других, из-за внешнеполитической ситуации усугубило проблему защиты персональных данных. В стремлении обойти блокировки, пользователи начали активно использовать различные VPN-сервисы, что позволило им создать иллюзию надежного зашифрованного подключения к Интернету. Однако это привлекло внимание мошенников. В частности, VPN-сервисы стали использоваться для разноплановового хищения персональных данных, так как они позволяют получать конфиденциальную информацию без ведома пользователя и распространять ее в незащищенной цифровой среде. Кроме того, при загрузке приложений, маскирующихся под VPN-сервисы, или перехода по ссылкам существует высокий риск установки вредоносного ПО и (или) взаимодействия с ним, способного передавать личные сведения пользователя третьим лицам. На фоне этих событий, крупные технологические компании начали разрабатывать новые методы защиты, включая использование искусственного интеллекта и машинного обучения для обнаружения и предотвращения киберугроз. Эти технологии позволяют более эффективно выявлять подозрительную активность на базе автономных протоколов и защищать пользователей от потенциальных атак.

Угроза утечки данных, несанкционированного доступа, нарушения приватности пользователей и злоупотребления личной информацией становится все более серьезной системой проблем, поскольку информационное пространство как многоуровневый технологический инструмент, который помогает достигать целей и выполнять задачи как отдельным лицам, так и организациям различного масштаба, включая государства [9], не только совершенствуется и усложняется, но становится одновременно в той или иной степени уязвимым. Поскольку, нужно понимать, что любое обновление имеет на какой-то период времени или (и) постоянной основе свои «лазейки». Утечка персональных данных масштабное явление последнего десятилетия, которое приносит исключительно негативные последствия. Несмотря на возможность как объективных технических, так и субъективных причин, например, халатность сотрудников или корыстные мотивы, персональные данные, попавшие в руки злоумышленников, могут быть использованы в преступных целях (займы, незаконные сделки с недвижимостью, денежные переводы и т.д.) [1].

Только в 2024 году Роскомнадзор зафиксировал 135 случаев утечек баз данных, содержащих более 710 миллионов записей о россиянах. По статистическим данным, опубликованным органом государственной власти, в 2022 году произошло около 150 крупных утечек персональных данных, из которых 87 % случаев факты незаконного распространения личной информации были подтверждены. В 2023 году Роскомнадзор зарегистрировал 168 утечек персональных данных, из-за которых в открытый доступ попало больше 300 млн записей о россиянах [11]. Как стало известно из СМИ к экспертам Центра правовой помощи гражданам в цифровой среде — создан по инициативе Роскомнадзора — в прошлом году обратились почти 1,7 тыс. заявителей. Большая часть обращений (52 %) касалась обработки личной информации без ведома и согласия человека, 16 % случаев связано от мошеннических действий с личными сведениями, 9 % — персональные данные использовались в рекламных целях без их согласия, а из 10 % случаев связаны с защитой гражданами своей чести, достоинства и деловой репутации. Э.Т. Халиулина в своей научной работе, рассуждая о причинах латентности, отмечает на основе статистических данных, что почти половина опрошенных прокуроров (43,1 %) указали на совершение преступлений в «виртуальной среде»; 39,2 % — на скрытость

для большинства населения, сложности выявления таких преступлений; 29,0 % — на создание новых IT-технологий; 28,3 % — на увеличение пользователей сети «Интернет» и мобильных компьютерных устройств[14].

Основными причинами, иллюстрирующими совершения противоправных деяний как с персональными данными, так и информационных преступлений в принципе, можно считать на данный момент: широкое распространение безналичных платежей, например, процветание и набирание оборота такой тенденции как осуществление купли-продажи на интернет-площадках; недостаточная подготовленность правоохранительных органов, что выражается в их неспособности оперативно реагировать на киберпреступления, эффективно проводить расследования в цифровой среде и отсутствие возможности адаптироваться к новым техническим вызовам; несовершенство законодательства, не исключение варианта избежать наказания или получить более мягкое IT-преступникам; слабо развитый механизм международного сотрудничества между правоохранительными органами и экспертами в различных странах; недостаточная осведомленность населения о рисках, связанных с использованием цифровых технологий [12]; социально-экономическое неравенство, которое наиболее ярко можно проследить в эпоху социальных сетей, преобладание медиа-контента от различных категорий населения и преуспевание развития инфоцыган, что способствует у некоторых групп людей видеть в преступлений в сфере компьютерной информации способ достижения материального благосостояния; для организаций можно выделить такие причины для благоприятного осуществления кибератак, в большинстве случаев именно на персональные сведения клиентов и (или) сотрудников компаний, как недостаточные инвестиции в обеспечении информационной безопасности, непроведение аудита и пентеста, слабая инфраструктура и недостаток осведомленности сотрудников о рисках и мерах предосторожности.

Проблемы, привлекающие внимание к изучению и рассмотрению персональных данных, обусловлены не просто актуальностью времени, но и их сложной структурой и технической спецификой, в частности речь идет о биометрических данных, которые имеют выраженный характер особенной характеристики внутреннего устройства и требующий не менее уникального подхода к организационному и правовому регулированию; невозможностью своевременной адаптации законодательства и его применителей к модернизирующемся механизмам преступлений; а также сомнительным и не соответствующим действительности содержанием дефиниции «компьютерная информация», суть которой раскрыта законодателем в примечании к ст.272 УК РФ, поскольку с ней связана теперь категория персональных данных по факту нововведения ст.272.1 УК РФ.

Статья 23 Конституции Российской Федерации гарантирует каждому право на защиту частной жизни, личной и семейной тайны, а также на охрану чести и доброго имени, что подчеркивает значимость защиты персональных данных, так как они являются неотъемлемой частью частной и личной жизни человека. Защита персональных данных считается одной из приоритетных задач государства и общества обеспечения информационной безопасности в рамках национальной не только из-за своей структурной специфики, а также масштаба последствий посягательства на такого рода информацию, но и наличия конституционной принадлежности. Во всех наших взаимодействиях мы используем информацию о себе, которая может варьироваться от паспортных данных и финансовых транзакций до генетических сведений и учетных записей. Эта информация формирует комплексный институт персональных данных, охватывающий как имущественные, так и личные характеристики конкретного человека. Законодатель не ограничивает объем идентифицирующей информации, поэтому такого рода сведения могут включать биографические детали и данные, возникающие в результате взаимодействия с государственными учреждениями, общественными и частными организациями на протяжении жизни индивида. Отсутствие любой конкретики способствует появлению дискуссий.

Одним из острых вопросов, существующей в доктрине, по праву можно считать, отнесение персональных данных к сведениям о частной жизни, личной и семейной тайн, которые подлежат из всех уровней защиты в том числе и конституционной. Суть проблемы заключается, что неопределенность их связей между собой этих понятий и персональных данных осложняет системное толкование законодательства и правоприменения, поскольку они как специальный объект защиты в Конституции РФ не упоминаются [3].

При дальнейшей характеристике сущности дефиниции «персональные данные» сквозь различные интерпретации будем придерживаться авторской позиции о том, что это самостоятельные категории, которые пересекаются в своем значении, но никак в содержании и объеме. Данное мнение основывается, во-первых, на понимании, что права человека на защиту персональных данных проистекают из его права на неприкосновенность частной жизни, во-вторых на восприятии сложной структуры персональных данных, а именно, на понимании специфики и самостоятельности тех видов сведений, которые она обобщает своей сутью идентификации личности, в-третьих, на разъяснении Судьи Конституционного Суда РФ Гаджиева Г.А.: «С точки зрения требований ч. 1 ст. 24 Конституции наиболее уязвимой является такая информация, по которой можно персонифицировать отдельную личность и которая находится вне пределов постоянного контроля данного лица. Законодательство

РФ выделяет информацию такого рода в отдельную категорию «персональные данные», которая хотя и пересекается с формулой «информация о частной жизни», но не вполне идентична ей» [6]. Поэтому невозможно не согласиться с М.И. Проскуряковой, которая констатирует, что охрана персональных данных непосредственно связана с такими конституционными правами человека, как право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, право на неприкосновенность жилища, а вышеперечисленные права образуют собой конституционно-правовые рамки защиты персональных данных [10, с. 15].

Для установления точных границ правомерной уголовно-правовой защиты персональных данных и недопущения нарушения права на неприкосновенность частной жизни необходимо иметь четкое определение того, что будет к ним относится.

Федеральный закон № 152-ФЗ «О персональных данных» (далее — Закон о персональных данных) урегулировал вопросы защиты личной информации и устанавливает права и обязанности как субъектов данных, так и операторов, обрабатывающих эти сведения. Однако стоит отметить, что законодатель разъяснил суть сведений такого рода через ориентир прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), что позволяет вести речь о содержательной вариативности как в доктрине, праве, так и практике.

Как было охарактеризовано нами ранее по своей сути в такие сведения включен один или несколько признаков человека, В.В. Вабищевич акцентирует на характерной их принадлежности к физической, психологической, умственной, экономической, культурной или социальной идентичности [2].

Нас непосредственно интересуют те типы личной информации, которые подпадают под уголовную защиту, а именно, перечень противоправных деяний с ними, который содержится в Особенной части УК РФ. Судебная практика по делам, связанными с персональными данными, основывалась до конца 2024 года исключительно на незаконном собирании или распространении сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространении этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации (ст.137 УК РФ), и тех случаях, когда само деяние, совершенное лицом затрагивало персональные данные или подразумевало в своем исполнении их завладение и использование для реализации преступного умысла (например, против семьи и несовершеннолетних (гл. 20 УК РФ),в сфере экономической деятельности (гл. 22 УК РФ), против интересов службы в коммерческих и иных организациях (гл. 23 УК РФ), против здоровья населения и общественной нравственности (гл. 25 УК РФ), преступления с использованием персональных данных в сфере компьютерной информации (гл. 28 УК РФ)). Например, Виничук П.В., Вронская М.В. выделяют такие конкретные известные нередкие случаи как доведение людей до самоубийства, распространение лживых сведений (клевета) в организациях, учебных учреждениях и т.д., вовлечение несовершеннолетних в собирание и продажу персональных данных физических лиц, что влечет за собой нарушение частной жизни граждан; владение чужими данными для пропаганды террористических действий, их подготовки и реализации; сбор, употребление и массовое распространение наркотических, психотропных веществ; вовлечение несовершеннолетних в занятие проституцией; распространение порнографических материалов, в частности с участием несовершеннолетних лиц; пробуждение всеобщей ненависти или вражды[4].

Ситуация изменилась произведенными изменениями в Уголовный кодекс Российской Федерации, а непосредственно в главу 28 УК РФ, Федеральным законом от 30.11.2024 № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации». Новая статья УК РФ, разработанная в Законопроекте № 502113-8 и прошедшая все стадии дополняет имеющийся перечень составов преступлений в сфере компьютерной информации.

Непосредственным объектом преступления является общественные отношения, обеспечивающие правомерное использование и (или) передачу (распространение, предоставление, доступ), сбор и (или) хранение компьютерной информации, содержащей персональные данные, самим создателем (владельцем), потребление ее иными пользователями. Предметом преступления выступает охраняемая законом (установлен специальный правовой режим, помимо данной статьи также Федеральным законом от 27 июля 2006 г. №152-ФЗ «О персональных данных» и рядом иных НПА) компьютерная информация, содержащая персональные данные.

При том, что складывается, на первый взгляд, впечатление о подмене понятий «персональные данные» и «компьютерная информация» с технической стороны (с текущей формулировкой невозможно не согласиться), однако в целях реализации целей уголовного закона отдать предпочтение данному закреплению не будет ошибкой, поскольку этимология использованной дефиниции законодателем охватывает две группы сразу. Семантический анализ «компьютерной информации, содержащей персональные данные» сводится к формулировке прямо или косвенно относящиеся к конкретному физическому лицу сведения, представленные в форме электрических сигналов независимо от средств их хранения, обработки и передачи в запоминающем устройстве электронно-вычислительных машин и в других компьютерных устройствах либо на любых внешних

электронных носителях (дисках, в том числе жестких дисках — накопителях, флеш-картах и т.п.) в форме, доступной восприятию компьютерного устройства, и (или) передаваться по каналам электрической связи. Это складывается из учета в совокупности таких правовых понятий как компьютерная информация, которая содержится в примечании к статье 272 УК РФ, и персональные данные из Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». Разберемся в сущности каждого из них. Согласно уголовному закону под компьютерной информацией понимаются любые сведения (сообщения, данные), представленные в виде электрических сигналов, независимо от средств их хранения, обработки и передачи.

По смыслу части 1 статьи 272 УК РФ в качестве охраняемой законом компьютерной информации рассматривается как информация, для которой законом установлен специальный режим правовой защиты, ограничен доступ, установлены условия отнесения ее к сведениям, составляющим государственную, коммерческую, служебную, личную, семейную или иную тайну (в том числе персональные данные), установлена обязательность соблюдения конфиденциальности такой информации и ответственность за ее разглашение, так и информация, для которой обладателем информации установлены средства защиты, направленные на обеспечение ее целостности и (или) доступности.

По отношению к ст.272.1 УК РФ взят исключительно элемент предмета касаемо персональных данных, что выделено теперь в отдельной статье. Последние в свою очередь подразумевают любые сведение, относящиеся прямо или косвенно к определенному или определяемому физическому лицу, а персональные данные, разрешенные субъектом для распространения подразумевают такую информацию, доступ к которой у неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом для распространения в порядке, предусмотренном настоящим Федеральным законом, который также констатирует цели, ориентировочный список сведений и условия, при которых персональные данные могут быть размещены в открытых источниках. К указанной информации относятся: фамилия, имя, отчество; год, месяц и дата рождения; место рождения; ИНН; адрес; телефон; семейное, социальное и имущественное положение; образование; профессия; занимаемая должность; стаж работы; доходы, а также другая информация (письмо Минкомсвязи России от 28.08.2020 N ЛБ-С-074-24059). Важно отметить, что абонентский номер и адрес электронной почты считаются персональными данными исключительно в отношении физических лиц. Если же они принадлежат юридическому лицу, такие данные не относятся к категории персональных. Так и получается, что по смыслу статьи Уголовного кодекса Российской Федерации, информация, касающаяся физического лица, даже в косвенной форме, способна оказывать воздействие на его конституционные права.

Часть вторая статьи 272.1 Уголовного кодекса Российской Федерации устанавливает ужесточенную уголовную ответственность за неправомерные действия в отношении персональных данных несовершеннолетних, а также специальной категории информации и биометрических данных.

В действующем законодательстве Российской Федерации отсутствуют специальные нормы, обеспечивающие безопасность и охрану персональных данных несовершеннолетних лиц. Перечень защищаемых данных для подобной категории граждан совпадает с перечнем для совершеннолетних лиц. Однако стоит учитывать позицию Министерства цифрового развития, связи и массовых коммуникаций России, которое полагает, что к персональным данным несовершеннолетних следует также относить информацию из свидетельства о рождении, а также данные, содержащиеся в личном деле ученика и классном журнале (письмо от 28.08.2020 ЛБ-С-074-24059).

К специальным категориям персональных данных относятся сведения о расовой и национальной принадлежности, политических взглядах, религиозных или философских убеждениях, здоровье, интимной жизни, а также информация о судимости, согласно пунктам 1 и 3 статьи 10 Закона о персональных данных. Эти данные могут использоваться исключительно для заранее определенных и законных целей, таких как медицинские исследования, статистические обработки или иные области, где такая информация необходима для достижения общественно значимых целей. Важно отметить, что субъекты данных имеют право на доступ к своей информации, ее исправление и удаление, что подчеркивает необходимость прозрачности и уважения к личной жизни.

Биометрические персональные данные, указанные также в юридической конструкции ст. 272.1 УК РФ, подразумевают такие сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (статья 11 Закона о персональных данных). Такие характеристики представляют собой набор сведений о физиологической природе человека с их личными индивидуальными особенностями, позволяющими из-за технической основы автоматически идентифицировать человека и производить аутентификацию и обработку его персональных данных по собственному желанию или при наличии письменного согласия субъекта, за исключением определенных случаев. Совершенно справедливо Г.Г. Камалова конкретизирует принадлежность к субъекту биометрических персональных данных через

дактилоскопическую, антропометрическую, габитологическую (признаки внешнего облика), генотипическую и иную информацию, а также строение папиллярных узоров, размеры тела и отдельных его частей, особенности внешнего облика (красная кайма губ, строение радужной сетчатки глаза, кровеносных сосудов глазного дна), особенности артикуляции речевого аппарата и голоса, походки, жестикуляции, мимики, письма и т.д. [5]

Сложный характер и двойственность определения биометрических данных не препятствует выделению их признаков как дефиниции. Рассмотрим градацию характеристик через технический и правовой подходы, так как они представляют основу сложной структуры подобного типа данных, что позволит вообразить особенности этих сведений, а также базируясь на чем из всего перечня персональных данных, можно вычленить из них нужный тип необходимо понимание технических характеристик (шифрование привычных информационных объектов в специальный код; средство аутентификации; наличие специализированного интерфейса; надежность верификации; индивидуальный механизм регистрации в базе для каждого вида биометрических данных; применение ключей для считывания; изменчивость видов данных биологически, но невозможность их изменить технически; оптимальные параметры разрешения и качества загружаемых физиологических сведений субъекта; алгоритмы обработки) и правовых признаков (защиты и обеспечения приватности граждан; регламентация случаев, когда согласие лица для обработки сведений не требуется; урегулированность ответственности за нарушение законодательства в области информационной безопасности, принцип прозрачности и минимизации, тесная связь с правом на защиту личной жизни[8]. Также они не утрачивают видовые признаки своих «прародителей» (биологических и поведенческих характеристик индивида): неотделимость от личности их обладателя; идеальный характер сведений; невозможность денежного восстановления (возмещения) объектов в случае посягательства на них; выполнение функции индивидуализации гражданина [7].

Таким образом, вопрос сущности персональных данных в уголовной сфере был представлен для дальнейшего изучения при учете нерешённых или менее значимых на данный момент аспектов. Однако в ближайшем будущем, благодаря теоретическим и практическим наработкам, эти проблемы смогут быть решены, и системы личной информации будут надёжно функционировать на цифровых платформах без страха ежеминутной уязвимости. При всех нюансах и противоречиях «свежего» состава в Особенную часть УК РФ пока делать выводы о пригодности или неработоспособности, предлагая изменения непосредственно в новеллу, ближайшие пару лет не совсем является правильным решением. Также многие люди не знают о масштабах возможных последствиях использования компьютерной информации для совершения преступлений, а другие не принимают достаточных мер для защиты своих данных. Это также создает благоприятную среду для развития киберпреступности и затрудняет борьбу с ней. Комплексные меры позволят создать надёжную и эффективную систему защиты информации, адаптированную к требованиям современного цифрового общества.

ЛИТЕРАТУРА

1. Буркова А.Ю. Определение понятия «персональные данные» // Право и экономика. — 2015. — № 4. — С. 20–24
2. Вабищевич В.В. Определение персональных данных в целях их уголовно-правовой охраны // Вестник Полоцкого государственного университета: научно-теоретический журнал. 2019. № 14. С. 137.
3. Войниканис Е.А., Машукова Е.О., Степанов-Егиянц В.Г. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о частной жизни и персональных данных: проблемы совершенствования законодательства // Законодательство: право для бизнеса. 2014. № 12. С. 77.
4. Вронская М.В. Биометрические данные как объект правовой охраны и защиты: актуальные проблемы / М.В. Вронская, П.В. Виничук // Международный научно-исследовательский журнал. — 2024. — № 4(142). — DOI 10.23670/IRJ.2024.142.109. — EDN KRKPGM.
5. Камалова Г.Г. Биометрические персональные данные: определение и сущность //Информационное право. 2016 № 3 С. 8–12.
6. Комментарий к Конституции Российской Федерации / Под ред. проф. В.Д. Зорькина — 3-е изд., пересмотр. — Москва: Норма: НИЦ ИНФРА-М, 2013. — 1040 с. ISBN 978-5-91768-441-3. — Текст: электронный. — URL: https://znanium.com/catalog/product/431466 (дата обращения: 08.01.2025). — Режим доступа: по подписке.
7. Крутий Е.А. Биометрические данные как объект гражданских прав / Е.А. Крутий // Научно-исследовательская деятельность в классическом университете: традиции и инновации: Материалы Международного научно-практического фестиваля, 15–29 апреля 2020 г. — Иваново: Ивановский государственный университет, 2020 г. — С. 516–519. — EDN UTDCOU
8. Пекарева В.В. Категории биометрических данных: правовой и технический подходы / В.В. Пекарева // Международный журнал гуманитарных и естественных наук. — 2024. — № 5-1(92). — С. 154–157. — EDN JOOPLA.
9. Пекарева, В. В. Характеристика цифровых прав: специфика и проблемное определение их содержания / В. В. Пекарева, В. В. Туарменский // Евразийский юридический журнал. — 2025. — № 3(202). — С. 513–515.
10. Проскурякова, М.И. Конституционно-правовые рамки защиты персональных данных в России / М.И. Проскурякова // Вестник СПбГУ. Сер. 14. Право. — 2016. — Вып. 2. — С. 12–27.
11. Роскомнадзор о состоянии утечек персональных данных. URL: https://t.me/rkn_tg/428 (дата обращения: 10.01.2025 г.).
12. Туарменский, В.В. Социология массовых коммуникаций / В.В. Туарменский. — Курск: ИД Университетская книга, 2022. — 156 с. — ISBN 978-5-907679-16-0. — EDN FSQMSQ.
13. Халиулина Э.Т. Преступления, совершаемые с использованием персональных данных: характеристика состояния // Военное право. — 2021. — № 2(66). — С. 289–294. — EDN QBXHIE.

© Пекарева Виктория Владимировна (viktoria.pekareva@yandex.ru)