

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ ЭКОНОМИКИ ДАННЫХ*

А.А. Шутова, И.Р. Бегишев, А.В. Волкова

Казанский инновационный университет имени В.Г. Тимирязова, г. Казань, Россия

Информация о статье

Дата поступления –

13 января 2026 г.

Дата принятия в печать –

20 марта 2026 г.

Дата онлайн-размещения –

20 июня 2026 г.

Ключевые слова

Персональные данные, экономика данных, уголовная ответственность, незаконный оборот персональных данных, информационная безопасность, состав преступления, цифровизация, криминализация, информационное общество

Изучена динамика законодательного регулирования ответственности за незаконный оборот персональных данных. Исследуется состав преступления, предусмотренный ст. 272¹ Уголовного кодекса РФ, проблемы установления объекта и предмета посягательства, квалификации деяния при конкуренции уголовно-правовых норм. Внимание уделяется соотношению уголовно-правовых механизмов охраны персональных данных с нормами смежных отраслей права. Формулируются предложения по совершенствованию системы уголовно-правовой охраны персональных данных в части уточнения признаков предмета преступления, разграничения со смежными составами, а также дифференциации уголовной ответственности с учетом специфики информационной среды и экономических интересов субъектов оборота данных. Делается вывод о том, что эффективная охрана персональных данных в условиях экономики данных требует не только совершенствования уголовного закона, но и выработки единого образного подхода в правоприменении.

CRIMINAL LAW PROTECTION OF PERSONAL DATA IN A DATA ECONOMY**

Albina A. Shutova, Ildar R. Begishev, Anna V. Volkova

Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia

Article info

Received –

2026 January 13

Accepted –

2026 March 20

Available online –

2026 June 20

Keywords

Personal data, data economy, criminal liability, illegal trafficking of personal data, information security, corpus delicti, digitalization, criminalization, information society

The article addresses a subject of acute contemporary significance: the criminal law protection of personal data under conditions of an emerging data economy.

The research hypothesis advanced by the authors posits that, while the enactment of Article 272¹ of the Criminal Code of the Russian Federation represents a qualitatively new stage in the evolution of criminal law protection of personal data, the legislative construction of this norm contains substantial conceptual and technical deficiencies that impede effective law enforcement and require systematic legislative correction. The stated aim of the study – to determine the mechanism of criminal law protection of personal data in a data economy, assess the effectiveness of the new legislative instrument, and formulate proposals for its improvement – is declared as fully achieved by the authors.

The methodological framework of the study integrates general scientific methods – dialectical, systemic-structural, formal-logical, analytical and synthetic approaches – with specialised legal methods, including comparative law, formal dogmatic analysis and statutory interpretation.

The principal results of the research are structured across several interrelated dimensions. First, the authors examine the legal nature of personal data as the subject matter of criminal offences, demonstrating that, within the data economy paradigm, personal information acquires characteristics fundamentally distinguishing it from traditional objects of legal protection: it may be reproduced, aggregated and enriched without apparent detriment to the original subject, which substantially complicates the criminal qualification of unlawful

* Статья подготовлена при стипендиальной поддержке Казанского инновационного университета имени В.Г. Тимирязова (ИЭУП).

** The article was prepared with the scholarship support of the Kazan Innovative University named after V.G. Timiryasov (IEML).

acts. Second, the paper provides a systematic analysis of the corpus delicti under Article 272¹, identifying the constituent elements of its subject matter – computer information, the personal data content thereof, and the illegal origin of such information – as a tripartite construct that is unique within Russian criminal law and demands careful doctrinal elaboration. Third, the authors critically examine the legislative placement of Article 272¹ within Chapter 28 of the Criminal Code (crimes in the sphere of computer information), arguing that the primary object of the offence is not computer security but rather the constitutional right of the individual to privacy, personal and family secrecy as guaranteed by Article 23 of the Constitution of the Russian Federation, thereby supporting the position that normative placement within Chapter 19 would be more doctrinally coherent. Fourth, the study conducts a rigorous analysis of qualification problems arising from competition between Article 272¹ and related criminal law provisions, including Articles 137, 183, 272 and 274¹ of the Criminal Code, proposing specific rules for resolving such conflicts in practice.

The authors propose a normative clarification of the concept of “illegal acquisition” of personal data by way of a cross-reference to the grounds established by Federal Law No. 152-FZ on Personal Data; and the introduction of an immunity provision within the footnotes to Article 272¹ for persons who voluntarily disclose unlawfully obtained data arrays, modelled on analogous incentive norms elsewhere in the Criminal Code.

1. Введение

Общество переживает масштабную трансформацию, обусловленную всеобщей цифровизацией экономических, социальных и политических процессов. Информация, прежде всего персональные данные физических лиц, превращается в центральный элемент хозяйственной деятельности, определяя конкурентоспособность субъектов рынка и формируя самостоятельный сегмент экономики – так называемую экономику данных. Данная модель хозяйственных отношений предполагает масштабный сбор, обработку, хранение и коммерческую эксплуатацию сведений о гражданах, что неизбежно порождает новые угрозы их правам и законным интересам [1]. Следует подчеркнуть, что ценность персональных данных как экономического актива неуклонно возрастает: на их основе выстраиваются механизмы таргетированной рекламы, кредитного скоринга, медицинской диагностики, а также всё более изощренные схемы мошенничества и иных преступных посягательств.

Показательна в этом отношении статистика: по сведениям аналитических компаний, в 2024 г. объем официально выявленных утечек персональных данных в России превысил 1,5 млрд записей, а суммарный экономический ущерб от подобных инцидентов исчислялся миллиардами рублей¹. Указанные цифры свидетельствуют о том, что незаконный обо-

рот персональных данных превратился в масштабное социально опасное явление, угрожающее не только правам отдельных граждан, но и устойчивости информационной инфраструктуры государства в целом. Более того, данные преступления нередко выступают инструментом реализации иных преступных посягательств – мошенничества, вымогательства, шпионажа, – что свидетельствует о высокой степени их общественной опасности.

Вопросы правовой охраны персональных данных неоднократно становились предметом научного обсуждения [2–5]. В 2024 г. Е.В. Хохловой защищена кандидатская диссертация по научной специальности 5.1.4 «Уголовно-правовые науки» на тему «Незаконные действия с персональными данными: уголовно-правовое исследование» [6]. Вместе с тем проблематика уголовно-правовых инструментов противодействия незаконному обороту персональных данных приобрела особую остроту лишь в последние годы – в связи с фундаментальными изменениями в системе как фактических угроз, так и правового регулирования в данной сфере. Отправной точкой для анализа следует считать Федеральный закон от 30 ноября 2024 г. № 421-ФЗ², которым гл. 28 Уголовного кодекса (далее – УК) РФ была дополнена ст. 272¹, криминализировавшей незаконный оборот компьютерной информации, содержащей персональные данные. Данный шаг законодателя вызвал

¹ InfoWatch: РФ заняла в 2024 году пятое место по числу утечек личных данных // ТАСС. 2025. 19 марта. URL: <https://tass.ru/obshchestvo/23439577> (дата обращения: 12.01.2026).

² Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» // Собрание законодательства Российской Федерации. 2024. № 49 (ч. IV). Ст. 7412.

широкую дискуссию и требует всестороннего теоретико-прикладного осмысления.

Проблема ответственности за незаконный оборот персональных данных вызывает особый интерес исследователей. Опубликовано множество работ, посвященных изучению нового состава преступления, предусмотренного ст. 272¹ УК РФ, а также проблем квалификации данного преступления [7–14]. И.С. Алихаджиевой опубликована серия работ, посвященных персональным данным как специфическим предметам преступлений [15–18]. Однако персональные данные в условиях экономики не изучались авторами детально и подробно.

Стоит обратить внимание на то, что значимой практики применения рассматриваемой уголовно-правовой нормы всё еще нет. Несмотря на то, что согласно данным МВД России, в I полугодии 2025 г. в России выявлено 601 преступление по ст. 272¹ УК РФ, по 313 из них возбуждены уголовные дела³, однако, согласно данным Судебного департамента при Верховном Суде РФ, за тот же период только по одному делу был осужден гражданин⁴. Считаем, что данное обстоятельство не должно препятствовать осмыслению состава преступления, предусмотренного ст. 272¹ УК РФ, для того чтобы сделать прогноз применения, который может быть полезен для практики.

Целью настоящего исследования является определение механизма уголовно-правовой охраны персональных данных в условиях экономики данных, включая оценку эффективности нового законодательного инструментария и выработку предложений по его совершенствованию.

2. Персональные данные в условиях экономики данных

Экономика данных представляет собой систему хозяйственных отношений, при которой сведения о физических лицах и иная информация выступают ресурсом производства стоимости, т. е. обладают самостоятельной экономической ценностью [19, с. 144–145]. Данная модель опирается на технологии больших данных, искусственного интеллекта и машинного обучения, позволяющие извлекать ком-

мерчески значимые инсайты из массивов персональной информации, собираемых в режиме непрерывного мониторинга поведения пользователей. Следует отметить, что в условиях экономики данных персональные данные приобретают черты, принципиально отличающие их от традиционных объектов правовой охраны: они могут быть воспроизведены, агрегированы и обогащены без явного ущерба для исходного «носителя», что существенно осложняет квалификацию противоправных действий с ними.

Статья 3 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Закон № 152-ФЗ)⁵ содержит весьма широкое определение персональных данных как «любую информацию, относящуюся к прямо или косвенно определенному либо определяемому физическому лицу». Отсутствие конкретного перечня сведений, которые относятся к персональным данным, приводит к тому, что к ним относят как прямо идентифицирующие сведения: имя, адрес, номер документа, – так и косвенные идентификаторы: биометрические данные, сетевые идентификаторы, геолокационные метки, поведенческие профили⁶. Указанная дефиниция обладает недопустимым уровнем законодательной абстракции, которая позволяет относить к рассматриваемой категории любую информацию, связанную с человеком [2, с. 12]. Отсутствие перечня сведений, относимых к персональным данным, поднимает вопрос об их отграничении от сведений о частной жизни лица, составляющей его личную или семейную тайну (предмет преступления, предусмотренного ст. 137 УК РФ) [3, с. 334].

В свою очередь предметом преступления, предусмотренного ст. 272¹ УК РФ, выступает не персональная информация как таковая, а компьютерная информация, содержащая персональные данные, полученная незаконным путем. В диспозиции уголовно-правовой нормы законодатель одновременно использует категориальный аппарат двух правовых режимов – информационного права и уголовного права, что порождает ряд квалификационных трудностей, которые будут рассмотрены далее.

³ За полгода выявили более 600 преступлений, связанных с оборотом персональных данных // RuBezh. 2025. 5 сент. URL: <https://ru-bezh.ru/zakonodatelstvo-i-normativyi/news/25/09/05/za-polgoda-vyyavili-bolee-600-prestupleniy-s-оборотом-personalnyy> (дата обращения: 12.01.2026).

⁴ Сводные статистические сведения о состоянии судимости в России за 1 полугодие 2025 года // Судебный департамент при Верховном Суде РФ: офиц. сайт. URL: <https://cdep.ru/index.php?id=79&item=9303> (дата обращения: 12.01.2026).

⁵ Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3451.

⁶ Разъяснения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30 августа 2013 г. «Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки» // СПС «Гарант».

Для целей правоприменения под компьютерной информацией, содержащей персональные данные, следует понимать числовые коды, пригодные для последующей обработки в информационно-телекоммуникационных системах, сетях и устройствах и позволяющие идентифицировать конкретного человека.

3. Система уголовно-правовой охраны персональных данных

До принятия Федерального закона от 30 ноября 2024 г. № 421-ФЗ⁷ уголовное законодательство обеспечивало охрану персональной информации граждан посредством ряда норм, расположенных в различных главах УК РФ, что подтверждалось сложившимся правоприменением, прежде всего ст. 137 УК РФ, предусматривавшей ответственность за незаконное соби́рание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну. Помимо этого, охранительные функции применительно к отдельным категориям персональных данных выполняли ст. 138, 155, 183, 272, 273 УК РФ, а также ряд других норм. Тем не менее указанные нормы не обеспечивали системной уголовно-правовой охраны персональных данных именно в их современном понимании, характерном для экономики данных. Статья 137 УК РФ ориентирована прежде всего на защиту тайны частной жизни в ее традиционном понимании и не охватывала многочисленные случаи массовой коммерческой «эксплуатации» персональных данных.

Значительный научный и практический интерес представляет ст. 272¹ УК РФ, устанавливающая запрет незаконного оборота компьютерной информации, содержащей персональные данные, законодательная конструкция которой содержит ряд неточностей и правовых неопределенностей, способных существенно осложнить ее практическое применение. В частности, требует уточнения понятие «незаконное получение персональных данных», поскольку именно это обстоятельство важно для квалификации последующих действий как преступных. При этом в Законе № 152-ФЗ предусмотрен значительный перечень оснований для законной обработки персональных данных без согласия их субъекта, что создает дополнительные трудности при разграничении правомерного и противоправного поведения в сфере оборота данных.

4. Состав преступления, предусмотренный ст. 272¹ УК РФ: дискуссионные вопросы

Правильное установление объекта и предмета преступления, предусмотренного ст. 272¹ УК РФ, приобретает особую значимость ввиду сложной правовой природы персональных данных и неоднозначности позиции законодателя в части структуры охраняемых правоотношений. Указанная норма помещена в гл. 28 УК РФ, что предполагает отнесение их родового объекта к общественной безопасности и общественному порядку (раздел IX УК РФ), а видового объекта – к общественным отношениям в сфере безопасного использования компьютерной информации. Однако незаконный оборот персональных данных прежде посягает на конституционное право граждан на неприкосновенность частной жизни, личную и семейную тайну, гарантированные ст. 23 Конституции РФ [20, с. 216]. В этом смысле компьютерная безопасность выступает лишь дополнительным объектом посягательства, тогда как основным следует признать конституционные права личности в информационной сфере. В доктрине многими авторами критикуется законодательное решение о расположении состава преступления в гл. 28 УК РФ, а не в гл. 19 [20, с. 216; 21, с. 124]. Однако другие специалисты высказываются о целесообразности размещения данного состава именно в гл. 28 УК РФ [22, с. 154]. Полагаем, что указанный вопрос носит теоретический характер и не будет оказывать сильного влияния на процесс правоприменения, несмотря на то, что мы придерживаемся позиции о том, что персональные данные как сведения о человеке не могут быть отделены от его личности, поэтому целесообразнее ответственность за незаконный оборот персональных данных было бы разместить в гл. 19 УК РФ. Кроме того, введение специального уголовно-правового запрета только из-за деления предмета преступления на виртуальный аналог физического предмета представляется не совсем корректным, поскольку и до установления ответственности за незаконный оборот персональных данных (ст. 272¹ УК РФ) уголовный закон позволял привлекать к ответственности лиц за совершение подобных деяний.

Предмет преступления, предусмотренного ст. 272¹ УК РФ, образует совокупность трех взаимосвязанных компонентов: во-первых, это компьютерная информация; во-вторых, она должна содержать

⁷ Федеральный закон от 30 ноября 2024 г. № 421-ФЗ «О внесении изменений в Уголовный кодекс Российской

Федерации» // Собрание законодательства Российской Федерации. 2024. № 49 (ч. IV). Ст. 7412.

персональные данные; в-третьих, эта информация должна быть получена незаконно. Следует указать, что подобная конструкция предмета, соединяющая в себе признаки компьютерно-технического и информационно-правового характера, в определенной степени уникальна для системы российского уголовного законодательства и требует внимательного доктринального осмысления. Следует ли ожидать введения, например, уголовно-правовой нормы за незаконный оборот компьютерной информации, содержащей коммерческую или государственную тайну? Документированные персональные данные не охраняются ст. 272¹ УК РФ, ответственность за посягательства на них обеспечивается прежними уголовно-правовыми нормами (ст. 137 УК РФ).

С практической точки зрения существенное значение приобретает вопрос о том, может ли предметом преступления по ст. 272¹ УК РФ выступать публично доступная персональная информация. Представляется, что при наличии иных признаков состава ответ должен быть утвердительным: факт общедоступности персональных данных не снимает вопроса о законности их первоначального получения и последующего оборота, поскольку Закон № 152-ФЗ допускает обработку общедоступных персональных данных лишь в определенных целях и в пределах их изначального раскрытия.

Объективная сторона состава преступления, предусмотренного ст. 272¹ УК РФ, представляет собой совокупность альтернативных действий с предметом преступления: незаконное использование, передача (распространение, предоставление, доступ), сбор и хранение компьютерной информации, содержащей персональные данные. Все перечисленные деяния согласно легальному определению относятся к разновидностям обработки персональных данных (ст. 3 Закона № 152-ФЗ). Таким образом, законодатель криминализировал определенные формы обработки персональных данных при условии, что сами данные были первоначально получены незаконным путем.

Полагаем необходимым выяснить содержание понятия «незаконность получения персональных данных», поскольку именно данный признак является системообразующим для квалификации деяния. Получение персональных данных считается законным в следующих случаях: при наличии согласия субъекта персональных данных, надлежащим образом оформленного в соответствии со ст. 9 Закона № 152-ФЗ; в случаях, прямо предусмотренных зако-

нодательством (например, для обеспечения правосудия, исполнения государственных полномочий, защиты жизни или здоровья); при получении данных надлежащим образом уполномоченным лицом в пределах своих компетенций. Соответственно, получение персональных данных незаконным путем охватывает все ситуации, при которых перечисленные условия не соблюдены: неправомерный доступ к информационным системам, получение данных путем обмана или принуждения, превышение пределов согласия субъекта и иные подобные действия.

Проблему представляет ситуация, при которой незаконный оборот персональных данных осуществляется легально функционирующей организацией, т. е. субъект, осуществляющий обработку определенного массива персональных данных, использует их за пределами установленных законом или договором целей (т. е. получил их на законных основаниях, но использует их не только в предусмотренных целях, но и, например, передает третьим лицам). Думается, что в случаях незаконного использования или распространения этих данных применение ст. 272¹ УК РФ невозможно.

Однако работники организаций, которые за вознаграждение «сливают» служебные базы данных с персональной информацией клиентов, могут выступать субъектами преступления, поскольку могут получить такую информацию в нарушение установленного нормативными правовыми актами порядка, независимо от формы такого доступа. В диспозиции уголовно-правовой нормы, закрепленной в ст. 272¹ УК РФ, «неправомерность происхождения» компьютерной информации как признак предмета преступления может быть обусловлена нарушением локальных правовых актов организации в сфере информационной (цифровой) безопасности, регламентирующих сам доступ к такой информации, в том числе цели такого доступа. Нарушение соответствующих положений указывает на неправомерное получение персональных данных гражданина, хранящихся в информационной системе организации. Соответственно, все возможные последующие деяния (использование, распространение и др.) содержат признаки состава преступления, предусмотренного ст. 272¹ УК РФ. Так, в период с февраля по июль 2025 г. сотрудница полиции, используя служебное положение и доступ к специальному программному резерву, осуществила незаконный сбор и передачу денежных данных о жителях Левокумского округа Ставропольского края. В отношении нее было возбуждено уголовное дело по

признакам состава преступления, предусмотренного п. «г» ч. 3 ст. 272¹ УК РФ, дело направлено в районный суд для рассмотрения по существу⁸.

5. Проблемы квалификации

Существенную проблему представляет квалификация преступлений по ст. 272¹ УК РФ в совокупности со смежными составами. Так, в ситуации, когда незаконный оборот персональных данных предшествует мошенническим действиям, содеянное должно квалифицироваться по ст. 159 и 272¹ УК РФ.

Вместе с тем необходимо принимать во внимание возможную конкуренцию со ст. 137, 183, 272 УК РФ, при которой подлежат применению общие правила преодоления конкуренции норм: приоритет специальной нормы над общей и нормы при конкуренции частей и целого. Учитывая, что ст. 272¹ УК РФ является специальной по отношению к ст. 272 УК РФ в части деяний с персональными данными и к ст. 137 УК РФ – в части компьютерной обработки информации, квалификация содеянного по совокупности указанных норм в большинстве случаев представляется излишней. В свою очередь посягательства на персональные данные в аналоговой форме влекут применение к лицу «традиционных» уголовно-правовых запретов.

Как совокупность преступлений, предусмотренных ст. 272¹ и 274¹ УК РФ, следует квалифицировать неправомерное собирание персональных данных посредством преодоления средств программно-технической защиты (взлома) – компьютерной атаки на значимые объекты критической информационной инфраструктуры Российской Федерации. Значительные объемы персональных данных граждан злоумышленники могут получить посредством неправомерного воздействия на информационные системы в сфере образования и здравоохранения. Так, сотрудник телекоммуникационной компании в Магаданской области, используя свое служебное положение, из личной заинтересованности совершил неправомерный доступ к охраняемой законом компьютерной информации, чем причинил вред критической информационной инфраструктуре Российской Федерации, а также осуществил незаконные сбор и распространение компьютерной информации, содержащей персональные данные граждан, исполь-

зующих услуги связи указанной телекоммуникационной компании. Гражданин признан виновным в совершении преступлений, предусмотренных п. «г» ч. 3 ст. 272¹, ч. 4 ст. 274¹ УК РФ⁹.

В ст. 272 УК РФ законодатель сделал оговорку, суть которой заключается в устранении возможной конкуренции. Однако, в отличие от ст. 272¹ УК РФ, состав преступления, предусмотренный ст. 272 УК РФ, сформулирован как материальный, и деяние признаётся оконченным в момент наступления общественно опасных последствий (копирование, блокирование, уничтожение, модификация). Следовательно, если лицо осуществило неправомерный доступ к объекту информационно-телекоммуникационной инфраструктуры организации, скопировало компьютерную информацию, содержащую персональные данные, а также осуществило модификацию или блокирование компьютерной информации, изменив идентификаторы доступа администратора ресурса или иным способом, то содеянное необходимо квалифицировать по совокупности преступлений, предусмотренных ст. 272 и 272¹ УК РФ. При этом если лицо только скопировало компьютерную информацию, содержащую персональные данные, оно фактически совершило в смысле ст. 272¹ УК РФ их сбор, в этом случае дополнительной квалификации по ст. 272 УК РФ не требуется.

В примеч. 1 к ст. 272¹ УК РФ указано, что действие статьи не распространяется на случаи обработки персональных данных физическими лицами исключительно для личных и семейных нужд. Е.А. Русскевич полагает, что законодатель формулирует своеобразный «универсальный критерий малозначительности» для того, чтобы исключить из сферы уголовной репрессии известные формы «бытового» распространения персональных данных близких, друзей, родственников и знакомых, когда лицо не утруждает себя тем, чтобы истребовать на это согласие субъекта персональных данных [14, с. 57–58]. Представляется, что решение связано с тем, что данные деяния не обладают той степенью общественной опасности, достаточной для привлечения лица к уголовной ответственности и явно не связаны с массовой коммерческой «эксплуатацией» персональных данных, носящей возмездный характер.

⁸ Прокуратура направила в суд уголовное дело о незаконном сборе и передаче персональных данных // Прокуратура Ставропольского края: офиц. сайт. 2025. 10 нояб. URL: https://epp.genproc.gov.ru/ru/proc_26/mass-media/news/regional/e6350874/ (дата обращения: 12.01.2026).

⁹ Сотрудника связи в Магадане поймали на утечке персональных данных // MagadanMedia. 2025. 5 марта. URL: <https://magadanmedia.ru/news/2418504/> (дата обращения: 12.01.2026).

6. Перспективы совершенствования российского законодательства

На основе проведенного исследования представляется возможным сформулировать следующие предложения по совершенствованию отечественного законодательства в области противодействия незаконному обороту персональных данных в условиях экономики данных:

- Во-первых, необходима трансформация диспозиции уголовно-правовой нормы, закрепленной в ст. 272¹ УК РФ, в части уточнения понятия «незаконное получение персональных данных» путем введения отсылки к основаниям, установленным Законом № 152-ФЗ. Подобное решение позволит устранить правовую неопределенность и обеспечит системное единство уголовно-правового и информационного законодательства.

- Во-вторых, необходимо дополнить примечание к ст. 272¹ УК РФ условием об освобождении от уголовной ответственности лиц, добровольно сообщивших об известных им массивах незаконно полученных персональных данных, – по аналогии с поощрительными нормами, предусмотренными в иных разделах УК РФ. Данная мера позволит расширить круг источников информации об утечках и будет способствовать раннему обнаружению фактов незаконного оборота персональных данных.

7. Заключение

Проведенное исследование позволяет сформулировать следующие выводы. Формирование экономики данных предопределило качественный рост общественной опасности деяний, связанных с незаконным оборотом персональных данных: будучи ценнейшим экономическим ресурсом, персональная информация граждан превратилась в желанный объект преступных посягательств, масштаб и изощренность которых непрерывно возрастают. Введение ст. 272¹ УК РФ знаменует качественно новый этап в развитии отечественной системы уголовно-правовой охраны персональных данных, впервые создан специальный уголовно-правовой инструмент противодействия данному явлению.

Вместе с тем анализ новой нормы выявил ряд проблем, требующих законодательного разрешения: неточность понятийного аппарата, сложность разграничения законного и незаконного оборота персональных данных, конкуренция со смежными составами преступлений.

Таким образом, принятый закон следует рассматривать как важный, но не окончательный шаг на пути к созданию комплексного и эффективного механизма уголовно-правовой охраны персональных данных в условиях экономики данных. Дальнейшее совершенствование данного механизма требует консолидации усилий законодателя, правоприменителей и научного сообщества.

СПИСОК ЛИТЕРАТУРЫ

1. Афанасьев С. Д. Правовое регулирование оборота данных: современные проблемы в контексте формирования экономики данных / С. Д. Афанасьев, Л. Т. Чихладзе // Закон и право. – 2024. – № 2. – С. 37–42. – DOI: 10.24412/2073-3313-2024-2-37-42.
2. Бегишев И. Р. Проблемные вопросы уголовно-правовой охраны персональных данных / И. Р. Бегишев, Д. В. Кирпичников // Уголовная юстиция. – 2020. – № 15. – С. 11–16. – DOI: 10.17223/23088451/15/3.
3. Шутова А. А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные / А. А. Шутова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. – № 4 (32). – С. 332–335.
4. Просветова О. Б. Защита персональных данных : автореф. дис. ... канд. юрид. наук / О. Б. Просветова. – Воронеж, 2005. – 22 с.
5. Белгородцева Н. Г. Теоретико-правовые аспекты защиты персональных данных : автореф. дис. ... канд. юрид. наук / Н. Г. Белгородцева. – М., 2012. – 25 с.
6. Хохлова Е. В. Незаконные действия с персональными данными: уголовно-правовое исследование : дис. ... канд. юрид. наук / Е. В. Хохлова. – Белгород, 2024. – 255 с.
7. Акинина Н. Ю. Криминализация незаконного оборота персональных данных / Н. Ю. Акинина, В. Ф. Анисимов, Р. В. Кочупалов // Вестник Сургутского государственного университета. – 2024. – Т. 12, № 3. – С. 84–91. – DOI: 10.35266/2949-3455-2024-3-8.
8. Щепельков В. Ф. Уголовная ответственность за незаконный оборот персональных данных (статья 272¹ Уголовного кодекса Российской Федерации) / В. Ф. Щепельков // Вестник Волгоградской академии МВД России. – 2025. – № 3 (74). – С. 35–42.

9. Стяжкина С. А. Вопросы квалификации незаконного оборота персональных данных / С. А. Стяжкина // Вестник Удмуртского университета. Серия Экономика и право. – 2025. – Т. 35, № 5. – С. 945–952. – DOI: 10.35634/2412-9593-2025-35-5-945-952.
10. Есаков Г. А. Незаконный оборот персональных данных (ст. 272.1 УК РФ) / Г. А. Есаков // Уголовное право. – 2025. – № 11 (183). – С. 10–17.
11. Чукреев В. А. Персональные данные, в том числе биометрические данные, как предметы уголовно-правовой охраны / В. А. Чукреев // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2022. – № 3. – С. 107–116. – DOI: 10.17803/2311-5998.2022.91.3.107-116.
12. Волкова А. В. Социальная обусловленность криминализации незаконных действий с компьютерной информацией, содержащей персональные данные / А. В. Волкова // Проблемы права. – 2025. – № 4 (100). – С. 86–95.
13. Князьков А. А. Уголовно-правовая новелла за нарушение законодательства о персональных данных (ст. 272¹ УК РФ): особенности конструирования состава и вопросы квалификации / А. А. Князьков // Вестник Университета имени О.Е. Кутафина (МГЮА). – 2025. – № 5. – С. 65–73. – DOI: 10.17803/2311-5998.2025.129.5.065-073.
14. Русскевич Е. А. Об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные / Е. А. Русскевич // Уголовный процесс. – 2025. – № 7 (247). – С. 53–59.
15. Алихаджиева И. С. Корыстная цифровая преступность с персональными данными / И. С. Алихаджиева // Проблемы правоохранительной деятельности на современном этапе : сб. тр. IV Всерос. (с междунар. участием) науч.-практ. конф. (Кострома, 24–25 апр. 2025 г.). – Кострома : Костром. гос. ун-т, 2025. – С. 167–173.
16. Алихаджиева И. С. Трансформация преступности, связанной с персональными данными / И. С. Алихаджиева // Вестник Прикамского социального института. – 2025. – № 2 (101). – С. 6–12.
17. Алихаджиева И. С. Криминологические риски персональных данных: основные тенденции и прогнозы / И. С. Алихаджиева // Известия Юго-Западного государственного университета. Серия: История и право. – 2023. – Т. 13, № 3. – С. 90–101. – DOI: 10.21869/2223-1501-2023-13-3-90-101.
18. Алихаджиева И. С. Частная жизнь, личная тайна или персональные данные: как толковать правоприменителю информацию о личности? / И. С. Алихаджиева // Известия Юго-Западного государственного университета. Серия: История и право. – 2024. – Т. 14, № 2. – С. 91–106. – DOI: 10.21869/2223-1501-2024-14-2-91-106.
19. Чан Фыок Тхинь. Экономика данных: барьеры, проблемы и решения / Чан Фыок Тхинь, Зыонг Кхань Чыонг, О. В. Староверова, О. А. Леонова // Экономика и управление: проблемы, решения. – 2025. – № 5 (158), Т. 9. – С. 142–155. – DOI: 10.36871/ek.ur.p.r.2025.05.09.017.
20. Алихаджиева И. С. Законопроект № 502113-8 «О внесении изменений в Уголовный кодекс РФ... (в части установления ответственности за незаконные использование и передачу, сбор и хранение компьютерной информации, содержащей персональные данные)»: научный комментарий / И. С. Алихаджиева // Уголовное право: стратегия развития в XXI веке. – 2024. – № 2. – С. 213–222.
21. Шутова А. А. Новеллы уголовного законодательства об ответственности за незаконный оборот персональных данных / А. А. Шутова // Ученые записки Казанского университета. Серия Гуманитарные науки. – 2024. – Т. 166, № 6. – С. 122–134. – DOI: 10.26907/2541-7738.2024.6.122-134.
22. Шагапсоев З. Л. К вопросу об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные / З. Л. Шагапсоев // Юридический вестник Дагестанского государственного университета. – 2025. – Т. 54, № 2. – С. 150–155. – DOI: 10.21779/2224-0241-2025-54-2-150-155.

REFERENCES

1. Afanasev S.D., Chikhladze L.T. Legal regulation of big data: modern problems in the context of the formation of the data economy. *Zakon i pravo = Law & Legislation*, 2024, no. 2, pp. 37–42. DOI: 10.24412/2073-3313-2024-2-37-42. (In Russ.).
2. Begishev I.R., Kirpichnikov D.V. Problems of personal data protection in criminal law. *Ugolovnaya yustitsiya = Russian Journal of Criminal Law*, 2020, no. 15, pp. 11–16. DOI: 10.17223/23088451/15/3. (In Russ.).

3. Shutova A.A. Social conditionality rules on the existence of criminal liability for the infringement of personal data. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal science and practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2015, no. 4 (32), pp. 332–335. (In Russ.).
4. Prosvetova O.B. *Personal data protection*, Cand. Diss. Thesis. Voronezh, 2005. 22 p. (In Russ.).
5. Belgorodtseva N.G. *Theoretical and legal aspects of personal data protection*, Cand. Diss. Thesis. Moscow, 2012. 25 p. (In Russ.).
6. Khokhlova E.V. *Illegal actions with personal data: criminal law research*, Cand. Diss. Belgorod, 2024. 255 p. (In Russ.).
7. Akinina N.Yu., Anisimov V.F., Kochupalov R.V. Criminalization of personal data illegal trade. *Vestnik Surgutskogo gosudarstvennogo universiteta = Surgut State University Journal*, 2024, vol. 12, no. 3, pp. 84–91. DOI: 10.35266/2949-3455-2024-3-8. (In Russ.).
8. Shchepelkov V.F. Criminal liability for illegal personal data trafficking (Article 272.1 of the Criminal Code of the Russian Federation). *Vestnik Volgogradskoi akademii MVD Rossii = Journal of the Volgograd Academy of the Ministry of the Interior of Russia*, 2025, no. 3 (74), pp. 35–42. (In Russ.).
9. Styazhkina S.A. Issues of qualification of illegal trafficking of personal data. *Vestnik Udmurtskogo universiteta. Seriya Ekonomika i pravo = Bulletin of Udmurt University. Series Economics and Law*, 2025, vol. 35, no. 5, pp. 945–952. DOI: 10.35634/2412-9593-2025-35-5-945-952. (In Russ.).
10. Esakov G.A. Illegal circulation of personal data (Art. 272.1 of the Criminal code of the Russian Federation). *Ugolovnoe pravo*, 2025, no. 11 (183), pp. 10–17. (In Russ.).
11. Chukreev V.A. Personal biometric data as subjects of criminal law protection. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) = Courier of Kutafin Moscow State Law University (MSAL)*, 2022, no. 3, pp. 107–116. DOI: 10.17803/2311-5998.2022.91.3.107-116. (In Russ.).
12. Volkova A.V. Social conditionality of criminalization of illegal actions with computer information containing personal data. *Problemy prava = Issues of law*, 2025, no. 4 (100), pp. 86–95. (In Russ.).
13. Knyazkov A.A. Criminal law novel for violation of the legislation on personal data (Art. 272¹ of the Criminal Code of Russia): design features of the composition and qualification issues. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) = Courier of Kutafin Moscow State Law University (MSAL)*, 2025, no. 5, pp. 65–73. DOI: 10.17803/2311-5998.2025.129.5.065-073. (In Russ.).
14. Russkevich E.A. On criminal liability for illegal actions with computer information containing personal data. *Ugolovnyi protsess*, 2025, no. 7 (247), pp. 53–59. (In Russ.).
15. Alikhadzhiyeva I.S. Self-serving digital crime with personal data, in: *Problemy pravookhranitel'noi deyatel'nosti na sovremennom etape*, Proceedings of the IV All-Russian (with international participation) scientific and practical conference (Kostroma, April 24–25, 2025), Kostroma, Kostroma State University Publ., 2025, pp. 167–173. (In Russ.).
16. Alikhadzhiyeva I.S. Transforming identity crime. *Vestnik Prikamskogo sotsial'nogo instituta = Bulletin of Prikamsky Social Institute*, 2025, no. 2 (101), pp. 6–12. (In Russ.).
17. Alikhadzhiyev I.S. Private Life, Personal Secret or Personal Data: How to Interpret Information about the Person to the Law Enforcement Officer?. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of Southwest State University. Series: History and Law*, 2023, vol. 13, no. 3, pp. 90–101. DOI: 10.21869/2223-1501-2023-13-3-90-101. (In Russ.).
18. Alikhadzhiyev I.S. Private Life, Personal Secret or Personal Data: How to Interpret Information about the Person to the Law Enforcement Officer?. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of Southwest State University. Series: History and Law*, 2024, vol. 14, no. 2, pp. 91–106. DOI: 10.21869/2223-1501-2024-14-2-91-106. (In Russ.).
19. Phuoc Thinh Tran, Khanh Truong Duong, Staroverova O.V., Leonova O.A. Data economy: barriers, problems, and solutions. *Ekonomika i upravlenie: problemy, resheniya*, 2025, no. 5 (158), vol. 9, pp. 142–155. DOI: 10.36871/ek.up.p.r.2025.05.09.017. (In Russ.).
20. Alikhajieva I.S. Bill № 502113-8 «On amending the Criminal Code of the Russian Federation (in the part of establishing responsibility for illegal use and transfer, collection and storage of computer information containing personal data)»: scientific comment. *Ugolovnoe pravo: strategiya razvitiya v XXI veke*, 2024, no. 2, pp. 213–222. (In Russ.).

21. Shutova A.A. Novelties in Russian criminal law on liability for personal data breaches. *Uchenye zapiski Kazanskogo universiteta. Seriya Gumanitarnye nauki = Kazan Journal of Historical, Linguistic, and Legal Research*, 2024, vol. 166, no. 6, pp. 122–134. DOI: 10.26907/2541-7738.2024.6.122-134. (In Russ.).

22. Shkhagapsoev Z.L. On the issue of criminal liability for illegal actions with computer information containing personal data. *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta = Law herald of Dagestan State University*, 2025, vol. 54, no. 2, pp. 150–155. DOI: 10.21779/2224-0241-2025-54-2-150-155. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Шутова Альбина Александровна – кандидат юридических наук, старший научный сотрудник Научно-исследовательского института цифровых технологий и права, доцент кафедры уголовного права и процесса
Казанский инновационный университет имени В.Г. Тимирязова
420111, Россия, г. Казань, ул. Московская, 42
E-mail: shutova1993@inbox.ru
SPIN-код РИНЦ: 5235-4319; AuthorID: 835100

Бегишев Илдар Рустамович – доктор юридических наук, доцент, заслуженный юрист Республики Татарстан, главный научный сотрудник Научно-исследовательского института цифровых технологий и права, профессор кафедры уголовного права и процесса
Казанский инновационный университет имени В.Г. Тимирязова
420111, Россия, г. Казань, ул. Московская, 42
E-mail: begishev@mail.ru
SPIN-код РИНЦ: 8859-9395; AuthorID: 595003

Волкова Анна Валерьевна – соискатель кафедры уголовного права и процесса
Казанский инновационный университет имени В.Г. Тимирязова
420111, Россия, г. Казань, ул. Московская, 42
E-mail: avmail555@gmail.com

БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Шутова А.А. Уголовно-правовая охрана персональных данных в условиях экономики данных / А.А. Шутова, И.Р. Бегишев, А.В. Волкова // Правоприменение. – 2026. – Т. 10, № 2. – С. 127–136. – DOI: 10.52468/2542-1514.2026.10(2).127-136.

INFORMATION ABOUT AUTHORS

Albina A. Shutova – PhD in Law; Senior Researcher, Institute of Digital Technologies and Law; Associate Professor, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: shutova1993@inbox.ru
RSCI SPIN-code: 5235-4319; AuthorID: 835100

Ildar R. Begishev – Doctor of Law, Associate Professor, Honored Lawyer of the Republic of Tatarstan; Chief Researcher, Institute of Digital Technologies and Law; Professor, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: begishev@mail.ru
RSCI SPIN-code: 8859-9395; AuthorID: 595003

Anna V. Volkova – applicant for PhD in Law, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: avmail555@gmail.com

BIBLIOGRAPHIC DESCRIPTION

Shutova A.A., Begishev I.R., Volkova A.V. Criminal law protection of personal data in a data economy. *Pravoprimenie = Law Enforcement Review*, 2026, vol. 10, no. 2, pp. 127–136. DOI: 10.52468/2542-1514.2026.10(2).127-136. (In Russ.).