

УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: <https://doi.org/10.60797/LAW.2026.9.3>

РАЗВИТИЕ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНЫЙ ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

Научная статья

Волкова А.Ю.^{1,*}¹ ORCID : 0000-0003-1944-3453;¹ Нижегородская академия МВД России, Нижний Новгород, Российская Федерация

* Корреспондирующий автор (auvolkovs[at]mail.ru)

Аннотация

Актуальность исследования динамики развития уголовной ответственности за неправомерный доступ к персональным данным личности не вызывает сомнения ввиду последних изменений уголовного законодательства, а также роста влияния информационно-телекоммуникационных технологий на расширение сфер применения персональных данных, соответственно, и их ценности. Потребность в урегулировании неправомерного доступа к личной информации возникла в связи с использованием подобной информации для совершения иных преступлений. По мнению автора, создание самостоятельной нормы за данное деяние позволит должным образом противодействовать уголовно-правовыми средствами фактам получения различных персональных данных, включая биометрические. В статье обосновывается необходимость применения уголовно-правовой нормы, устанавливающей ответственность за неправомерный доступ к персональным данным, в совокупности с действующим профильным информационным законодательством.

Ключевые слова: персональные данные, уголовная ответственность, преступление, уголовная политика, защита прав личности, информационная безопасность.

EXTENDING CRIMINAL LIABILITY FOR ILLEGAL ACCESS TO PERSONAL DATA

Research article

Volkova A.Y.^{1,*}¹ ORCID : 0000-0003-1944-3453;¹ Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia, Nizhny Novgorod, Russian Federation

* Corresponding author (auvolkovs[at]mail.ru)

Abstract

The relevance of researching the dynamics of criminal liability for illegal access to personal data is beyond doubt, given recent changes in criminal law and the growing influence of information and telecommunications technologies on the expansion of the scope of personal data use and, accordingly, its value. The need to regulate unlawful access to personal information arose in relation to the use of such information to commit other crimes. In the author's opinion, the creation of a separate norm for this act will make it possible to properly counteract, by means of criminal law, the acquisition of various types of personal data, including biometric data. The paper substantiates the need to apply a criminal law provision establishing liability for unlawful access to personal data, in conjunction with the existing relevant information legislation.

Keywords: personal data, criminal liability, crime, criminal policy, protection of individual rights, information security.

Введение

В последнее время динамичность развития информационно-телекоммуникационных технологий и их применения во всех сферах общественной жизни намного опережают развитие законодательства по отдельным вопросам повсеместной цифровизации. И зачастую совершенствование правового регулирования происходит постфактум после возникновения резонансных случаев противоправного поведения, которые наглядно демонстрируют недостаточность законодательных мер. Подобная ситуация складывается в сфере охраны правомерного доступа к персональным данным (далее — ПД) как к серьезному информационному блоку, используемому для реализации преступных намерений.

Неправомерный доступ к ПД является одной из наиболее актуальных угроз информационной безопасности в современном обществе, ввиду сопряженности с иными преступлениями, в большинстве случаев имущественного характера. Для наглядного представления степени общественной опасности посягательств на ПД как охраняемую законом информацию необходимо обратиться к официальной статистике, публикуемой МВД России. Так, за последние пять лет количество зарегистрированных преступлений, связанным с неправомерным доступом к компьютерной информации, которая включает в себя охраняемые ПД, характеризуется беспрецедентным ростом:

- 2019 г. — 2 420 преступлений;
- 2020 г. — 4 105 преступлений;
- 2021 г. — 6 392 преступления;
- 2022 г. — 9 308 преступлений;
- 2023 г. — 36 788 преступлений;
- 2024 г. — 105 311 преступлений.



За январь–декабрь 2025 г. зарегистрировано 58782 преступлений, предусмотренных ст. 272 УК РФ [1]. Отрицательная динамика объясняется введением самостоятельной нормы, устанавливающей ответственность за посягательство в отношении ПД личности [2].

Но расследование подобных преступлений связано с анонимностью и высокотехнологичностью их совершения, что затрудняет привлечение виновных к уголовной ответственности: согласно информации о количестве осужденных лиц за совершение деяния, предусмотренного ст. 272 УК РФ, к уголовной ответственности привлекается около 3% и менее, в зависимости от конкретного временного периода [3].

Официальная статистика в части роста количества случаев неправомерного доступа к компьютерной информации и общего количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий, наглядно демонстрирует потребность законодательного реагирования на неправомерный доступ к ПД. В связи с изданием Федерального закона от 30.11.2024 г. № 421-ФЗ в УК РФ была введена ст. 272, которая определяет информацию, содержащую ПД в качестве самостоятельного объекта уголовно-правовой охраны. Это в перспективе позволит обеспечить надлежащий уровень противодействия распространению данной охраняемой законом информации, в том числе посредством блокирования информационных ресурсов, предназначенных для ее хранения и (или) распространения. Федеральным законом от 31.07.2025 № 282-ФЗ были введены дополнительные составы, направленные на недопущение использования аккаунтов пользователей на различных информационных ресурсах и передачи абонентских номеров с нарушениями законодательства РФ. Названные изменения направлены на борьбу с преступлениями, сопряженными с использованием персональных данных личности, цифровых аккаунтов, что позволяет анонимизировать личность преступника в условиях глобальной цифровизации.

Ввиду последних изменений уголовного законодательства, хотелось бы отследить динамику становления ПД как самостоятельного объекта уголовно-правовой охраны и уголовной ответственности за неправомерный доступ к персональным данным, что наглядно продемонстрирует соответствие правового регулирования тем или иным реалиям цифровизации общественной жизни.

Основные результаты

Первоначально законодательное регулирование в области охраны ПД начало развиваться в 90-х гг. XX в., когда стало очевидно, что информационные технологии несут не только пользу, но и создают угрозы для личной безопасности и неприкосновенности частной жизни. С изданием Постановления Верховного Совета России от 23 сентября 1992 г. № 3524-1 в рамках отечественного правового поля появились такие личные права как право на имя и право на неприкосновенность (имеется ввиду неприкосновенность баз данных от посягательств, способных нанести ущерб чести и достоинству автора) [4]. В начале 90-х гг. ввиду разработки нового российского уголовного закона ранее действовавший уголовный закон не был дополнен самостоятельной нормой, предусматривающей ответственность за посягательство в отношении ПД как самостоятельного объекта уголовно-правовой охраны.

Законодательно ПД как самостоятельная категория были определены в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ в качестве сведений о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность [5]. Данным законом ст. 11 ПД были отнесены к категории конфиденциальной информации. Исчерпывающе конфиденциальная информация и сведения, ее составляющие, определяются Указом Президента РФ от 6 марта 1997 г. № 188. ПД являются первой категорией, которая приводится в данном Указе, и хотелось бы отметить, что данный нормативный источник является ныне действующим [6].

Вышеуказанные нормативные источники устанавливали общие принципы защиты информации, включая персональные данные, конкретные аспекты обработки и защиты данных, отдельные требования к техническим и организационным мерам безопасности. Но не конкретизировались меры ответственности за нарушения режима защиты, обработки и порядка использования этой информации. В зависимости от сферы использования ПД (врачебная, коммерческая, семейная, налоговая тайна и т.п.) деяние по разглашению ПД могло повлечь все виды юридической ответственности. Исходя из сложившегося правового режима ПД по вступившему в законную силу УК РФ 1996 г. ответственность за противоправные действия в отношении них могла наступать по ст. ст. 137, 183 и 272 УК РФ.

Следующим этапом развития ПД как самостоятельной категории правовой охраны стало принятие Федерального закона «О персональных данных» в 2006 г., который установил основные правила работы с информацией, содержащей личные сведения граждан. Но как бы не совершенствовалось законодательство, устанавливающее правовой статус ПД и обязанности операторов по их обработке, единообразного подхода к юридической ответственности за неправомерный доступ к ПД не сложилось: могли все также применяться ст. ст. 137, 183, 272 УК РФ. И с момента издания Федерального закона «О персональных данных» ряд ученых высказались о специфике и разрозненности реализации уголовной ответственности за неправомерный доступ к ПД, а также о необходимости создания самостоятельной нормы, однако разнились взгляды на ее место в уголовном законе [7, С. 11–16], [8, С. 151], [9, С. 16].

Коллизия, действующая продолжительный промежуток времени, в части применения ст. 137 и 272 УК РФ за неправомерный доступ к ПД, могла бы быть разрешена посредством формы представления данной информации. Если персональные данные представлены в форме сведений, представленных в форме электрических сигналов, то следовало применять ст. 272 УК РФ. Но это исключало бы создание самостоятельной нормы за посягательства в отношении ПД как самостоятельного объекта уголовно-правовой охраны.

Усиление внимания законодателя к обеспечению охраны ПД происходило постепенно: от создания норм, устанавливающих административную ответственность за ненадлежащее исполнение обязанностей по обеспечению сохранности ПД (например, ст.13.11 – 13.14 КоАП РФ) до установления требований к оценке вреда, который может быть причинен субъектам ПД в случае нарушения Федерального закона «О персональных данных» [10]. Актуальные изменения законодательства направлены на усиление уголовной ответственности за неправомерный доступ к ПД,



признавая преступлением не только непосредственные действия в отношении ПД, но и их трансграничное перемещение, а также поддержание информационных ресурсов, заведомо предназначенного для незаконного доступа к ПД (сайты в сети «Интернет», телеграм-каналы и боты и т.п.).

На настоящий специфика действия уголовно-правовой нормы, устанавливающей ответственность за неправомерный доступ к ПД, определяется формой их фиксации — исключительно в виде компьютерной информации. Если же ПД данные содержатся, например, на бумажных носителях, то также сохраняется практика применения норм иных статей уголовного закона в части нарушения особого режима охраны ПД. Различные правовые режимы конфиденциальности ПД обосновывают то, какие общественные отношения пострадали в результате противоправного деяния.

Основания криминализации посягательств в отношении ПД можно свести к юридико-криминологическим и к социально-экономическим. Первую группу оснований можно раскрыть следующим образом:

- распространённость деяний и динамика кратного роста с каждым годом;
- создания возможности воздействия на них уголовно-правовыми средствами при отсутствии возможности борьбы иными мерами.

Вторую группу оснований первостепенно составляет причиняемый деяниями ущерб и недостаточность превентивных мер, включая негативные последствия в рамках существующих уголовно-правовых запретов.

Обе названные группы оснований криминализации комплексно реализуют развитие уголовной ответственности за неправомерный доступ к ПД в современных реалиях. Но для эффективной реализации введенной нормы нужно исходить из специфики ПД и уже существующего режима охраны, предусмотренного действующим профильным информационным законодательством. И некоторые авторы отмечают, что применение норм об уголовной ответственности за неправомерный доступ к ПД может стать основанием для несогласованной правоприменительной практики и нуждается в дальнейших исследованиях института уголовной ответственности за незаконные действия с компьютерной информацией, содержащей ПД [11, С. 41], [12, С. 150–155].

Заключение

Координирование правовых предписаний, принимаемых в последнее время в отношении обработки ПД, определяет бланкетный характер введенной нормы не только в части преступных действий, но и оценки ущерба и тяжести возможных последствий. Например, Требования по оценке вреда, который может быть причинен субъектам ПД, утвержденные приказом Роскомнадзора от 27 октября 2022 г. № 178, могут быть имплементированы в Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 в части установления причиненного ущерба и соотношения с тяжестью последствий, наступивших в результате неправомерного использования этих данных. Согласно вышеуказанным Требованиям, оператор организации обработки ПД устанавливает одну из степеней вреда, который может быть причинен их владельцу в случае нарушения законодательства о ПД: высокая, средняя и низкая степень вреда [13]. Высокая и средняя степени вреда субъекту ПД напрямую соотносятся с тяжкими последствиями как квалифицирующим признаком в ст. ст. 272 – 274 УК РФ, описываемыми в п. 14 Постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37. Комплексное применение имеющихся законодательных предписаний и разъяснений судебной практики обеспечит надлежащую квалификацию посягательств в отношении ПД как самостоятельного объекта уголовно-правовой охраны.

Последние изменения уголовного законодательства направлены в частности на борьбу с использованием чужих SIM-карт и аккаунтов для обхода идентификации при совершении противоправных действий. Об эффективности реализации данных положений пока говорить рано, но законодатель комплексно подходит к обеспечению информационной безопасности личности, общества и государства в целом.

Таким образом, развитие уголовной ответственности за неправомерный доступ к ПД — это сложный и многогранный процесс, который направлен на защиту прав граждан в условиях возрастающих угроз информационной безопасности. Совершенствование законодательства и формирование единообразной практики его применения играют ключевую роль в обеспечении неприкосновенности персональных данных и сохранении доверия общества к цифровым технологиям. И чтобы гарантировать единство законодательных предписаний при обеспечении надлежащего уровня уголовно-правовой охраны ПД, необходимо учитывать иные нормативные источники, позволяющие установить факт неправомерных действий с ПД и степень причиненного вреда в части возможного ущерба или иных тяжких последствий.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Информация о состоянии преступности на территории Российской Федерации : данные ГИАЦ МВД России. — URL: <https://мвд.рф/reports> (дата обращения: 30.12.2025).
2. О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон № 421-ФЗ от 30.11.2024 г. / Собрание законодательства РФ. — 2024. — № 49 (часть IV). — Ст. 7412.



3. Информационный портал «Судебная статистика РФ» / Агентство правовой информации. — URL: <https://stat.апи-пресс.рф> (дата обращения: 30.12.2025).
4. Ведомости Съезда Народных Депутатов Российской Федерации и Верховного Совета Российской Федерации. — 1992. — № 42. — Ст. 2326.
5. Об информации, информатизации и защите информации : Федеральный закон № 24-ФЗ от 20.02.1995 (ред. от 10.01.2003) (утратил силу) / Собрание законодательства РФ. — 1995. — № 8. — Ст. 609.
6. Об утверждении Перечня сведений конфиденциального характера : Указ № 188 от 06.03.1997 (ред. от 13.07.2015) / Собрание законодательства РФ. — 1997. — № 10. — Ст. 1127.
7. Бегишев И.Р. Проблемные вопросы уголовно-правовой охраны персональных данных / И.Р. Бегишев, Д.В. Кирпичников // Уголовная юстиция. — 2020. — № 15. — С. 11–16.
8. Кудашкин Я.В. Правовое обеспечение безопасности обработки персональных данных в сети Интернет : дис. ... канд. юрид. наук / Я.В. Кудашкин. — Москва, 2019. — 199 с.
9. Хохлова Е.В. Незаконные действия с персональными данными: уголовно-правовое исследование : дис. ... канд. юрид. наук / Е.В. Хохлова. — Саратов, 2024. — 255 с.
10. Об утверждении Требований к оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»: Приказ № 178 от 27.10.2022 г. / Официальный интернет-портал правовой информации. — URL: <http://pravo.gov.ru> (дата обращения: 30.12.2025).
11. Щепельков В.Ф. Уголовная ответственность за незаконный оборот персональных данных (статья 272.1 Уголовного Кодекса Российской Федерации) / В.Ф. Щепельков // Вестник Волгоградской академии МВД России. — 2025. — № 3(74). — С. 35–42.
12. Шхагапсоев З.Л. К вопросу об уголовной ответственности за незаконные действия с компьютерной информацией, содержащей персональные данные / З.Л. Шхагапсоев // Юридический вестник Дагестанского государственного университета. — 2025. — № 2. — С. 150–155.

Список литературы на английском языке / References in English

1. Informatsiya o sostoyanii prestupnosti na territorii Rossiyskoy Federatsii [Information on the state of crime in the Russian Federation] : data from the Main Information and Analytical Center of the Ministry of Internal Affairs of Russia. — URL: <https://мвд.рф/reports> (accessed: 30.12.2025). [in Russian]
2. O vnesenii izmeneniy v Uголовnyy kodeks Rossiyskoy Federatsii [On amendments to the Criminal Code of the Russian Federation] : Federal Law No. 421-FZ of November 30, 2024 / Collection of Legislation of the Russian Federation. — 2024. — № 49 (part IV). — Art. 7412. [in Russian]
3. Informatsionnyy portal «Sudebnaya statistika RF» [Information portal "Judicial Statistics of the Russian Federation"] / Legal Information Agency. — URL: <https://stat.апи-пресс.рф> (accessed: 30.12.2025). [in Russian]
4. Vedomosti S'ezda Narodnykh Deputatov Rossiyskoy Federatsii i Verkhovnogo Soveta Rossiyskoy Federatsii [Gazette of the Congress of People's Deputies of the Russian Federation and the Supreme Soviet of the Russian Federation]. — 1992. — № 42. — Art. 2326. [in Russian]
5. Ob informatsii, informatizatsii i zashchite informatsii [On information, informatization and information protection] : Federal Law No. 24-FZ of February 20, 1995 (as amended on January 10, 2003) (repealed) / Collection of Legislation of the Russian Federation. — 1995. — № 8. — Art. 609. [in Russian]
6. Ob utverzhdenii Perechnya svedeniy konfidentsial'nogo kharaktera [On approval of the List of confidential information] : Decree No. 188 of March 6, 1997 (as amended on July 13, 2015) / Collection of Legislation of the Russian Federation. — 1997. — № 10. — Art. 1127. [in Russian]
7. Begishev I.R. Problemye voprosy ugovovno-pravovoy okhrany personal'nykh dannykh [Problematic issues of criminal law protection of personal data] / I.R. Begishev, D.V. Kirpichnikov // Uголовnaya yustitsiya [Criminal justice]. — 2020. — № 15. — P. 11–16. [in Russian]
8. Kudashkin Ya.V. Pravovoe obespechenie bezopasnosti obrabotki personal'nykh dannykh v seti Internet [Legal support for the security of personal data processing on the Internet] : dissertation for the degree of Candidate of Legal Sciences / Ya.V. Kudashkin. — Moscow, 2019. — 199 p. [in Russian]
9. Khokhlova E.V. Nezakonnyye deystviya s personal'nymi dannymi: ugovovno-pravovoe issledovanie [Illegal actions with personal data: criminal law research] : dissertation for the degree of Candidate of Legal Sciences / E.V. Khokhlova. — Saratov, 2024. — 255 p. [in Russian]
10. Ob utverzhdenii Trebovaniy k otsenke vreda, kotoryy mozhet byt' prichinen sub'ektam personal'nykh dannykh v sluchae narusheniya Federal'nogo zakona «O personal'nykh dannykh» [On approval of the Requirements for assessing the harm that may be caused to personal data subjects in case of violation of the Federal Law "On Personal Data"] : Order No. 178 of October 27, 2022 / Official Internet portal of legal information. — URL: <http://pravo.gov.ru> (accessed: 30.12.2025). [in Russian]
11. Shchepelkov V.F. Uголовnaya otvetstvennost' za nezakonnyy oborot personal'nykh dannykh (stat'ya 272.1 Uголовnogo Kodeksa Rossiyskoy Federatsii) [Criminal liability for illegal trafficking of personal data (Article 272.1 of the Criminal Code of the Russian Federation)] / V.F. Shchepelkov // Vestnik Volgogradskoy akademii MVD Rossii [Bulletin of the Volgograd Academy of the Ministry of Internal Affairs of Russia]. — 2025. — № 3(74). — P. 35–42. [in Russian]
12. Shkhagapsoev Z.L. K voprosu ob ugovovnoy otvetstvennosti za nezakonnyye deystviya s komp'yuternoy informatsiey, soderzhashchey personal'nye dannye [On the issue of criminal liability for illegal actions with computer information containing personal data] / Z.L. Shkhagapsoev // Yuridicheskiy vestnik Dagestanskogo gosudarstvennogo universiteta [Legal Bulletin of Dagestan State University]. — 2025. — № 2. — P. 150–155. [in Russian]