

УДК 343.1:342.7:004.9

DOI <https://doi.org/10.32782/apdp.v107.2025.4>*Д. А. Біленець, П. В. Шевчук*

ПРОБЛЕМИ КОЛІЗІЙ КРИМІНАЛІСТИЧНИХ ПРОЦЕДУР І ПРАВОМ НА ПРИВАТНІСТЬ І ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

Вступ. Активне впровадження цифрових технологій у криміналістику докорінно трансформує процес збирання, обробки та використання доказової інформації. Разом із цим зростає ризик порушення права людини на приватність, яке є фундаментальною конституційною гарантією. Використання біометричних і генетичних даних, цифрових слідів, інформації з мобільних пристроїв та хмарних сервісів створює складний баланс між інтересами правосуддя та необхідністю захисту персональних даних. Колізії між нормами кримінального процесу, конституційними гарантіями і міжнародними стандартами дедалі частіше виявляються у практиці органів досудового розслідування.

Проблематика правомірності втручання у приватне життя набуває особливої актуальності у зв'язку з цифровізацією слідчої діяльності, коли технічні можливості значно випереджають рівень нормативного регулювання. У сучасній правозастосовній практиці фіксуються випадки надмірного збору інформації, відсутності належних процесуальних гарантій, порушення принципу пропорційності та невизначеності меж допустимого використання персональних даних під час кримінального провадження. Ці тенденції посилюють потребу у виробленні єдиного підходу до гармонізації криміналістичних процедур із конституційним правом на приватність.

Аналіз останніх досліджень і публікацій. Питання співвідношення криміналістичних процедур і права на приватність знайшли відображення у працях українських дослідників, зокрема Гиляки О., Степанюка Р., Макарової О., Ратнової А. Науковці звертають увагу на проблеми нормативної невизначеності під час застосування технічних засобів фіксації, використання біометричних і цифрових даних, збирання доказів із соціальних мереж та електронних комунікацій. У працях Гаделії В. та Тимощука С. наголошується на колізіях між положеннями Конституції України і Кримінального процесуального кодексу, що створює ризики безпідставного втручання у приватну сферу особи.

У науковій літературі відсутнє системне дослідження комплексного характеру колізій між криміналістичними процедурами, цифровими технологіями та правом на приватність у контексті процесуальних гарантій. Ця прогалина зумовлює потребу у новому теоретико-прикладному осмисленні проблеми, орієнтованому на узгодження норм права з технологічними реаліями ХХІ століття.

Метою статті є визначення сутності та причин колізій між криміналістичними процедурами і правом на приватність, аналіз чинних нормативно-правових механізмів захисту персональних даних у кримінальному провадженні та формулювання пропозицій щодо удосконалення правового регулювання у цій сфері.

Наукова новизна статті полягає у спробі системного узагальнення видів і причин колізій між криміналістичними процедурами та правом на приватність, а також у визначенні напрямів нормативного узгодження між положеннями Конституції України, Кримінального процесуального кодексу та міжнародних актів.

Виклад основного матеріалу. Право на приватність належить до кола фундаментальних природних прав людини і становить основу захисту особистої сфери від свавільного втручання держави. Конституція України закріплює, що права та свободи людини визначають зміст і спрямованість діяльності держави, гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції та невтручання в особисте і сімейне життя, включно із захистом персональних даних [9].

З позиції розвитку національної правової системи ключовим спеціальним актом є Закон України «Про захист персональних даних», який встановлює правила обробки, передачі та зберігання даних [15]. Кримінальний процесуальний кодекс України визначає процедури доступу до речей і документів, тимчасового вилучення та арешту майна, проведення обшуку й негласних слідчих дій [11]. Нормативна база створює формальні рамки допустимого втручання органів досудового розслідування у приватну сферу людини.

На міжнародному рівні базовим орієнтиром залишається стаття 8 Європейської конвенції з прав людини, яка гарантує повагу до приватного та сімейного життя [6]. Важливу роль відіграє практика Європейського суду з прав людини: у справі *Klassand Others v. Germany* (1978) Суд наголосив, що таємне спостереження допустиме лише за умов ефективного демократичного контролю [2], а у справі *Big Brother Watchand Others v. United Kingdom* (2021) дійшов висновку, що масове перехоплення даних без достатніх процесуальних гарантій порушує статтю 8 Конвенції [1].

). Ці рішення задають стандарти пропорційності та необхідності, яким мають відповідати національні правові механізми.

Важливим є дотримання принципу цільового збору персональних даних. Ряд авторів підкреслили, персональні дані, зібрані для різних цілей, не повинні об'єднуватися, крім випадків, коли зазначені цілі є сумісними, а склад персональних даних, необхідний для досягнення обох цілей, збігається [3, с. 37]. Цей підхід повністю узгоджується з вимогами статті Загального регламенту ЄС про захист даних [7].

У контексті безпекових викликів, зокрема під час воєнного стану, гарантії приватності залишаються актуальними. В науковій літературі зазначається, що право особи на приватне життя, включно з конфіденційністю спілкування, гарантовано як на рівні національного законодавства, так і міжнародних актів, ратифікованих Україною [14, с.333]. Це підкреслює, що навіть за умов воєнних загроз держава не може повністю нівелювати гарантії приватності.

Проблеми ще більше ускладнює впровадження сучасних технологій обробки даних. Гиляка О. слушно зауважував, що оцінка загроз недоторканості приватного життя стає складнішою у зв'язку з розвитком алгоритмів штучного інтелекту та машинного навчання, адже навіть обмежений обсяг персональних даних зда-

тен розкривати іншу інформацію про особу, поширення якої вона не передбачала [5, с. 25]. Це свідчить про необхідність постійного оновлення нормативної бази для врахування нових технологічних ризиків.

Право на приватність у правовій державі вимагає не лише конституційного та законодавчого закріплення, а й створення ефективного механізму пропорційності втручання та судового контролю за доступом до персональних даних. Це стає особливо важливим у світлі цифровізації криміналістики та глобалізації потоків даних, коли традиційні підходи до регулювання потребують переосмислення.

Сучасна криміналістика активно використовує інструменти, які безпосередньо зачіпають приватну сферу людини. Вони забезпечують ефективність доказової діяльності, проте водночас створюють ризики надмірного та непропорційного втручання у приватне життя. Проблема полягає у пошуку балансу між публічним інтересом у розкритті злочинів і захистом фундаментальних прав людини.

Особливе місце серед таких процедур посідає збирання та використання біометричних і генетичних даних. ДНК-профілі, відбитки пальців, технології розпізнавання облич дають змогу швидко та надійно ідентифікувати осіб, причетних до тяжких злочинів. Проте втручання в біологічну сферу особи потребує суворих процесуальних гарантій. Степанюк вказував, що корисним для України може стати досвід Німеччини та Нідерландів, де масове ДНК-тестування на стадії досудового розслідування здійснюється лише за попереднім дозволом слідчого судді, із залученням осіб за їхньою письмовою згодою, а отримані біологічні зразки підлягають знищенню після одержання профілю та завершення розслідування [18, с. 246]. Такий підхід забезпечує дотримання принципу пропорційності втручання, зменшуючи ризик порушення приватності.

Цифрові криміналістичні процедури, такі як доступ до мобільних пристроїв, хмарних сховищ, електронної пошти та месенджерів, суттєво розширили можливості слідчих органів. Проте вилучення та обробка великих обсягів даних нерідко призводять до збирання інформації, що не має значення для конкретного провадження. Ратнова А. зазначала, що уряди країн визнають необхідність боротьби з кіберзлочинністю у глобальному масштабі, створюють спеціалізовані підрозділи та розвивають цифрову криміналістику, проте ефективно протидіяння кіберзлочинності потребує глибокого розуміння масштабів та впливу злочинності у кіберпросторі [17, с. 165]. Це свідчить, що технологічний прогрес вимагає оновлення як правових, так і методологічних підходів до захисту приватності.

Використання технічних засобів спостереження – відеокамер, GPS-трекінгу, прослуховування комунікацій – підсилює доказову базу, але створює ризик перетворення таких інструментів на засіб необмеженого контролю. Кримінальний процесуальний кодекс України регламентує їхнє застосування під час тимчасового доступу до речей і документів, тимчасового вилучення, арешту майна, домашнього арешту з використанням електронних засобів контролю та затримання особи без ухвали слідчого судді [11].

Поляк Ю. підкреслював, що технічні засоби доцільно застосовувати лише у випадках, коли цього вимагають конкретні процесуальні завдання, і лише під контролем суду [13, с. 124].

Традиційні слідчі дії також залишаються чутливими з точки зору захисту приватності. Коваленко зауважував, що під час проведення огляду дозволяється «оглядати і вилучати речі і документи, які мають значення для кримінального провадження», а під час обшуку – «оглядати і вилучати документи, тимчасово вилучати речі, які мають значення для кримінального провадження» [8, с. 286]. У практиці це положення іноді тлумачать надто широко, що призводить до втручання у приватну сферу осіб, не причетних до кримінального провадження.

На думку Макарової, забезпечення процесуальних прав учасників кримінального провадження передбачає не лише формальні норми, а й застосування науково обґрунтованих методів і стандартів, які гарантують законність і об'єктивність проведення слідчих дій, зокрема допитів, обшуків, оглядів місця події, а також належне використання технічних засобів фіксації доказової інформації [12, с. 257]. Дотримання цих стандартів є критично важливим для забезпечення допустимості доказів і захисту прав людини.

Впровадження цифрових технологій змінює саму природу доказового процесу. Крижановський А. слушно зауважив, що інформаційні технології та існуючий обіг цифрових даних здатні усунути суб'єктивний характер сприйняття інформації при доведенні обставин скоєння злочину [10, с. 828]. Проте залучення таких інноваційних засобів, як OSINT-докази із соціальних мереж, створює потребу у визначенні чітких процесуальних правил їхньої фіксації та оцінки. Радейко Р. зазначав, що дослідження фіксації OSINT-доказів на основі конкретних судових прецедентів дає змогу забезпечити гармонійне співіснування традиційних правових інститутів із технологічними рішеннями [16, с. 107].

Криміналістичні процедури, що зачіпають приватність, потребують комплексного підходу, який поєднує сучасні технологічні можливості та суворі правові гарантії. Забезпечення пропорційності втручання, мінімізації збору надлишкових даних і підвищення рівня судового контролю має стати ключовим напрямом удосконалення доказової діяльності у правовій державі.

Сучасна доказова діяльність у кримінальному процесі дедалі частіше стикається з конфліктом між потребами ефективного збирання доказів і гарантіями права на приватність. Проблема полягає не лише у наявності нових технологій, а й у неузгодженості законодавчих норм та практики їхнього застосування, що створює ризики порушення прав людини.

Однією з ключових колізій є розбіжності між нормами Конституції України та Кримінального процесуального кодексу. Тимошук вважав, що межі можливого застосування норми статті 31 Конституції України у контексті санкціонованого втручання у приватне спілкування значно ширші, ніж аналогічні приписи КПК, що створює передумови для безпідставного втручання у приватність особи [19, с. 192]. Така колізія свідчить про необхідність гармонізації конституційних положень та процесуального законодавства для уникнення правової невизначеності.

Не менш серйозною є проблема фактичного доступу до персональних даних у ході кримінального провадження. Гаделія В. підкреслював, що отримання доступу слідчими органами часто здійснюється через звичайний запит слідчого чи оперативного співробітника без дотримання обов'язкових умов, не кажучи

вже про отримання доступу через ухвалу слідчого судді [4, с. 516]. Це свідчить про розрив між нормами закону та їх практичною реалізацією, що може призвести до порушення гарантій захисту приватності.

Колізії між криміналістичними процедурами та правом на приватність мають комплексний характер і зумовлені як нормативними прогалинами, так і недосконалістю практики. Технологічний прогрес загострює ці суперечності, підвищуючи ризики порушення принципу пропорційності втручання. Вирішення цих проблем вимагає гармонізації законодавства, посилення судового контролю та запровадження чітких гарантій захисту приватності у процесі кримінального провадження.

Висновки. Захист приватності у кримінальному провадженні є фундаментальною гарантією правової держави та одним із ключових елементів довіри суспільства до системи правосуддя. Наявні колізії між конституційними нормами, положеннями КПК та фактичною практикою свідчать про необхідність їхнього узгодження. Лише за умови чіткого законодавчого врегулювання й реального судового контролю можливо досягти балансу між ефективністю криміналістичних процедур і дотриманням прав людини.

Гармонійне поєднання сучасних технологічних можливостей із принципами прав людини стане основою для справедливого та ефективного правосуддя. Розвиток криміналістики має відбуватися з урахуванням потреб суспільства та вимог верховенства права, що сприятиме не лише результативності доказової діяльності, а й підвищенню довіри громадян до державних інституцій у цифрову добу.

Література

1. Big Brother Watch and Others vs. The United Kingdom (Applications Nos. 58170/13, 62322/14 and 24960/15). URL: <https://hudoc.echr.coe.int/eng?i=001-210077>
2. CASE OF KLAS AND OTHERS v. GERMANY URL: <https://hudoc.echr.coe.int/eng?i=001-57510>
3. Бем М., Городиський І., Саттон Г., Родіоненко О. Захист персональних даних: правове регулювання та практичні аспекти. Київ: К.І.С., 2015, 220 с. URL: <https://rm.coe.int/168059920c>
4. Гаделія В. Р. Конституційно-правове забезпечення права на приватність при розслідуванні кримінальних правопорушень. Альманах права, 2024, вип. 15: 515–520, URL: <http://jnas.nbu.gov.ua/article/UJRN-0001525946>
5. Гиляка О. С. Право на приватність та захист персональних даних в умовах цифровізації. Вісник НАПрН України, 2023, 30 (1): 15–30. URL: <https://visnyk.kh.ua/uk/journals/visnik-naprn-1-2023-r/pravo-na-privatnist-ta-zakhist-personalnikh-danikh-v-umovakh-tsifrovizatsiyi>
6. Європейська конвенція з прав людини. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text
7. Загальний регламент про захист даних (GDPR), URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
8. Коваленко А. В. Криміналістичне вчення про збирання, дослідження та використання доказів у кримінальному провадженні: монографія. Київ: Алерта, 2024, URL: https://alerta.kiev.ua/img/cms/PDF/Kovalenko_mono_Zmist.pdf?srsltid=AfmBOoFFkUmnmZ0ymFFfvsEI0btoRj5IEgkjVsXaJGnK8zP-L3GEsKF
9. Конституція України: Закон України від 28.06.1996, № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
10. Крижановський А. С. Місце та роль інформаційних технологій у криміналістиці. Аналітично-порівняльне правознавство, 2024, 6: 824–829, URL: <https://app-journal.in.ua/wp-content/uploads/2024/12/139.pdf>
11. Кримінальний процесуальний кодекс: Закон України від 13.04.2012 № 4651-VI. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>

12. Макарова О. П. Забезпечення процесуальних прав учасників кримінального провадження на етапі досудового розслідування: теоретико-правовий і криміналістичні аспекти. *Вісник Кримінологічної асоціації України*, 2025, 35(2): 254–262, с. 257, DOI: <https://doi.org/10.32631/vsa.2025.2.19>
13. Поляк Ю. П. Застосування технічних засобів при проведенні слідчих (розшукових), негласних слідчих (розшукових) дій та використання його результатів під час досудового розслідування. Дисертація. Львів: ЛДУВС, 2022, 230 с. URL: <https://dspace.lvduvs.edu.ua/handle/1234567890/4812>
14. Привиденцев О., Артюх В., Бадов С. Втручання у приватне спілкування в рамках кримінального провадження: новели законодавства, пов'язані із введенням воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право*, 2025, 3.88: 329–334, URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/330836>
15. Про захист персональних даних: Закон України URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
16. Радейко Р. І. Теоретико-правові засади фіксації OSINT-доказів із соціальних мереж: процесуальні вимоги та методологічні підходи (на прикладі справи № 990/232/24). *Scientific notes of Lviv University of Business and Law*, 2025, 45: 110–116. URL: <https://nzlupb.org.ua/index.php/journal/article/download/1657/1436/>
17. Ратнова А. В. Кримінальні процесуальні та криміналістичні основи використання електронних документів у доказуванні. Дисертація на здобуття ступеня доктора філософії. Львів: ЛДУВС, 2021. URL: https://dspace.lvduvs.edu.ua/bitstream/1234567890/3747/1/ratnova_d.pdf
18. Степанюк Р. Л. Напрями вдосконалення правового регулювання криміналістичного ДНК-аналізу в Україні в контексті інтеграції до ЄС. *Вісник Харківського національного університету внутрішніх справ*, 2022, № 2(97): 234–249, с. 246, DOI: <https://doi.org/10.32631/v.2022.2.21>
19. Тимошук С. О. Забезпечення права на приватність у кримінальному провадженні: теоретичний і прикладний аспекти. Київ: Юридична думка, 2024, с. 192–193.

Анотація

Біленець Д. А., Шевчук П. В. Проблеми колізії криміналістичних процедур із правом на приватність і захист персональних даних. – Стаття.

У статті здійснено комплексне дослідження проблем колізії між криміналістичними процедурами та правом на приватність у контексті забезпечення захисту персональних даних особи. Підкреслюється, що активна цифровізація слідчої діяльності, впровадження штучного інтелекту, біометричних технологій, систем відеоспостереження, OSINT-підходів та електронного документообігу докорінно змінюють природу доказового процесу в Україні.

Розкрито конституційно-правову природу права на приватність як фундаментальної гарантії, що визначає межі державного контролю над громадянином. Проаналізовано положення Конституції України, Кримінального процесуального кодексу, Закону України «Про захист персональних даних», а також міжнародно-правові акти, зокрема статтю 8 Європейської конвенції з прав людини та Загальний регламент ЄС про захист даних (GDPR).

У статті доведено, що чинне українське законодавство не забезпечує належного балансу між інтересами правосуддя та правом особи на недоторканність приватного життя. Виявлено основні колізії між конституційними нормами, процесуальними положеннями КПК та практикою їх застосування під час слідчих і негласних слідчих дій. Особливу увагу приділено проблемам безконтрольного доступу до персональних даних, надмірного збору цифрової інформації, неврегульованості порядку використання біометричних і генетичних матеріалів. Зазначено, що навіть у воєнних умовах держава не звільняється від обов'язку гарантувати мінімальні стандарти приватності та пропорційності втручання.

Обґрунтовано необхідність уніфікації підходів до застосування технічних засобів контролю, запровадження судового дозволу на доступ до цифрових даних, знищення надлишкових біологічних зразків після завершення розслідування, а також посилення інституційної відповідальності за неправомірне використання персональної інформації. Запропоновано концепцію гармонізації криміналістичних процедур із міжнародними стандартами захисту приватності через інтеграцію принципів пропорційності, законності, технологічної нейтральності та підзвітності органів досудового розслідування.

У роботі підкреслено, що забезпечення реального балансу між безпековими потребами держави та особистими правами громадян є визначальною умовою зміцнення правової держави і довіри суспільства до системи правосуддя у цифрову добу.

Ключові слова: криміналістика, персональні дані, криміналістичні процедури, цифрові технології, біометрична інформація, судовий контроль, захист прав людини, OSINT.

Summary

Bilenets D. A., Shevchuk P. V. Problems of the collision of forensic procedures with the right to privacy and protection of personal data. – Article.

The article provides a comprehensive analysis of the conflicts between forensic procedures and the right to privacy in the context of ensuring the protection of personal data. It emphasizes that the active digitalization of investigative activities, the introduction of artificial intelligence, biometric technologies, video surveillance systems, OSINT methodologies, and electronic document management have fundamentally transformed the nature of the evidentiary process in Ukraine.

The paper reveals the constitutional and legal nature of the right to privacy as a fundamental guarantee defining the limits of state control over the individual. It analyzes the provisions of the Constitution of Ukraine, the Criminal Procedure Code, the Law of Ukraine “On Personal Data Protection,” as well as key international legal instruments, including Article 8 of the European Convention on Human Rights and the EU General Data Protection Regulation (GDPR).

The study demonstrates that current Ukrainian legislation does not provide an adequate balance between the interests of justice and the individual’s right to the inviolability of private life. The author identifies the main conflicts between constitutional norms, procedural provisions of the Criminal Procedure Code, and their practical implementation during investigative and covert investigative actions. Special attention is paid to the problems of uncontrolled access to personal data, excessive collection of digital information, and the lack of clear regulation for the use of biometric and genetic materials. It is noted that even under martial law, the state remains bound by its obligation to guarantee minimum standards of privacy and proportionality of interference.

The article substantiates the necessity of unifying approaches to the use of technical means of surveillance, introducing mandatory judicial authorization for access to digital data, ensuring the destruction of excessive biological samples after the completion of an investigation, and strengthening institutional responsibility for the unlawful use of personal information. The author proposes a conceptual model for harmonizing forensic procedures with international privacy protection standards through the integration of the principles of proportionality, legality, technological neutrality, and accountability of pre-trial investigation bodies.

The research concludes that maintaining a real balance between the state’s security needs and individual rights is a key precondition for consolidating the rule of law and strengthening public trust in the justice system in the digital age.

Key words: forensics, personal data, forensic procedures, digital technologies, biometric information, judicial control, human rights protection, OSINT, GDPR, proportionality.

Дата надходження статті: 19.09.2025

Дата прийняття статті: 14.10.2025

Дата публікації: 27.11.2025