УДК 343.13
DOI 10.33244/2617-4154.1(22).2026.167-174

В. О. Романов,
кандидат юридичних наук,
Сумська філія Харківського національного університету внутрішніх справ
email: romanovv.o.13@gmail.com
ORCID 0000-0002-8569-5723

НЕВИКОРИСТАНІ МАТЕРІАЛИ НСРД: РЕЖИМ, ЗНИЩЕННЯ, КОНТРОЛЬ

Негласні слідчі (розшукові) дії (далі – НСРД) передбачають негласне втручання в приватне життя. За таких умов особа, щодо якої здійснюється втручання, не має змоги одразу перевірити його законність або скористатися процесуальними гарантіями. Тому приватність залежить не лише від того, чи були НСРД належно санкціоновані, а й від того, що стається з отриманими матеріалами далі: як їх відбирають, де і як зберігають, хто має доступ, чи можливе повторне використання та за яких процедур дані стають реально недоступними. Водночас значна частина відомостей, зібраних під час НСРД, не набуває доказового значення або не долучається до провадження, але все одно може існувати як документ, річ, носій тощо.

У цифровому середовищі небезпека пов'язана не тільки зі збереженням, а й зі здатністю даних «відтворюватися» через дублікати й службові сліди – резервні копії, журнали доступу, синхронізовані сховища. До того ж у багатьох системах «видалення» є радше логічною операцією: зміст може залишатися в інших шарах зберігання або в резервних контурах. Отже, знищення має спиратися на перевірювані процедури, а не на одну технічну дію.

Мета статті – розкрити зміст спеціального режиму невикористаних матеріалів НСРД, окреслити типові ризики його реалізації в умовах цифровізації та запропонувати прикладні рішення, що підвищують підзвітність і роблять знищення фактичним. Для цього застосовано формально-юридичний аналіз приписів щодо знищення, заборони стороннього доступу й використання, повернення речей / документів і повідомлення осіб; системний підхід до гарантій приватності; а також функціональний аналіз організаційно-технічних бар'єрів (рольовий доступ, аудит, контроль копіювання й експорту). Використано підходи ЄСПЛ і висновки досліджень про безпечне видалення даних та надійність цифрових доказів.

Запропоновано типологію невикористаних матеріалів НСРД (протоколи / додатки; носії; речі та документи; похідні матеріали) і показано, що спеціальний режим має охоплювати весь обіг чутливих даних, а не обмежуватися питанням їхнього доказового статусу. У цифровому контексті «знищення» доцільно трактувати як доведений стан фактичної недоступності змісту та припинення обігу даних; цього не досягти

без інвентаризації місць зберігання, обліку копій і резервів та належного документування виконання. Так само заборони стороннього використання працюють лише тоді, коли їх підкріплено механізмами контролю – розмежуванням ролей, логуванням, аудитом, обмеженням копіювання та експорту.

Як прикладні рішення, запропоновано мінімальний стандарт реквізитів постанови прокурора про знищення (ідентифікація об'єктів без розкриття змісту; місця зберігання; окремий блок щодо копій / резервів; строк; відповідальні; спосіб контролю), уніфікований акт знищення цифрових даних із фіксацією охоплення резервів / синхронізацій, а також формалізацію повернення майна через акт приймання-передачі із зазначенням долі копій. Окремо наголошено на регулярних аудитних процедурах доступу до чутливої інформації як базовому стандарті підзвітності.

Ключові слова: *НСРД, невикористані матеріали, знищення інформації, цифрові дані, прокурорський контроль, приватність, аудит доступу, резервні копії, рольовий доступ, повернення речей.*

Постановка проблеми. НСРД як інструмент досудового розслідування пов'язані з інтенсивним втручанням у приватне життя [3]. Їхній негласний характер створює дефіцит прозорості: під час втручання особа не може швидко перевірити законність обмеження прав або скористатися засобами захисту. Тому потребує уваги оцінка не тільки до підстав санкціонування, а й до того, що відбувається після завершення НСРД: як організовано доступ, зберігання, використання та знищення отриманих матеріалів [10; 11]. У працях щодо масового перехоплення комунікацій підкреслюється, що саме правила «життєвого циклу» даних (доступ – зберігання – використання – знищення) є частиною стандарту запобіжників у системах негласного спостереження [10].

Практика показує, що помітна частина матеріалів НСРД не використовується в провадженні через відсутність доказової цінності, дублювання, зміну версій, припинення провадження або недоцільність подальшої обробки. Проте навіть «невикористаний» масив даних, якщо він залишається доступним, підтримує ризики витоку, несанкціонованого копіювання чи стороннього використання.

Кримінальний процес встановлює окремі правила для матеріалів НСРД, які прокурор не визнає відповідними: такі матеріали мають бути виведені з подальшого обігу, а будь-які дії з ними поза цілями кримінального провадження є неприпустимими; доступ до них має бути максимально обмеженим. Окремо врегульовано повернення речей / документів і повідомлення осіб про проведення НСРД [4]. Водночас цифрове середовище ускладнює виконання цих приписів: дані здатні «застрягати» у резервних контурах, логах або синхронізованих копіях, тому вимога «знищити» потребує процедурної перевірюваності [5]. Оглядові дослідження з безпечного видалення даних демонструють, що без інвентаризації місць зберігання та охоплення резервних контурів неможливо гарантувати фактичну недоступність інформації, навіть якщо «файл видалено» в робочій системі [5].

Аналіз останніх досліджень і публікацій. Проблему «надлишкових» даних після застосування негласних заходів зазвичай описують у двох взаємопов'язаних площинах. Перша – конвенційна та правозахисна: ідеться про критерії «якості закону», достатність запобіжників і контроль у режимах спостереження та перехоплення, включно з правилами доступу, зберігання й знищення [6; 10; 12]. Друга – техніко-процесуальна: ризики для справедливості провадження через складність цифрових доказів, множинність копій і нестачу процесуальних гарантій, адаптованих до цифрової реальності [7–9]. У межах цієї другої площини автори також наголошують, що оцінювання надійності цифрових процедур має спиратися на документованість і відтворюваність, а не лише на довіру до інституційного процесу [9].

Окремий масив робіт стосується «безпечного видалення» та помилки, коли видалення ототожнюють із фактичним знищенням: у багатьох системах операція видалення змінює лише доступність через інтерфейс, тоді як зміст може зберігатися і відновлюватися з резервів або похідних матеріалів [2; 5]. Водночас відкритим залишається питання, як перетворити правову вимогу «знищити» на перевірювану процедуру, яка охоплює копії / резерви й водночас не провокує розкриття чутливого змісту. У близькому контексті аналіз проваджень ЄСПЛ звертає увагу, що надмірна закритість здатна «вимивати» контроль, і тому мінімальна процедурна підзвітність має ключове значення навіть тоді, коли зміст матеріалів не може бути розкритий [6].

Мета статті – розкрити зміст правового режиму невикористаних матеріалів НСРД, окреслити ризики його реалізації в цифровому середовищі та запропонувати практично орієнтовані рішення, що забезпечують реальне (а не суто формальне) знищення й підзвітність процедур.

Виклад основного матеріалу. Спеціальний режим невикористаних матеріалів НСРД доцільно розуміти як гарантійний механізм постконтролю. Його логіка проста: надлишкові відомості не мають перетворюватися на автономний ресурс для процесуально несанкціонованого використання. Нормативно режим пов'язаний із прокурорською оцінкою «необхідності»: якщо матеріали не потрібні для подальшого розслідування, їх треба вивести з обігу так, щоб унеможливити подальше використання та доступ сторонніх осіб [4].

Важливо й те, що об'єктом режиму є не лише «докази», а ширший масив – відомості, речі та документи. У цифрових процесах це має особливе значення: чутливий зміст може відтворюватися в похідних файлах (витягах, транскриптах, довідках) або технічних копіях, які формально не є «доказом», але, по суті, містять приватну інформацію.

Для практики доцільно виокремлювати:

– протоколи та додатки (аудіо / відео / фото, метадані);
– носії / архіви (серверні записи, сховища, фізичні носії);
– речі та документи (отримані / вилучені / скопійовані у зв'язку з НСРД);
– похідні матеріали (витяги, транскрипти, аналітичні довідки).

Цей поділ важливий, бо «знищення» для кожної групи означає різні дії. Для паперових документів можливе комісійне знищення з оформленням акта. Натомість для цифрових даних ключовими стають інвентаризація місць зберігання, контроль резервів і синхронізацій,

а також документальне підтвердження того, що охоплено копії [2; 5]. Як показують роботи про безпечне видалення, саме неохоплені резервні контури та похідні матеріали найчастіше руйнують ідею «остаточного» знищення [2; 5]. Для речей і документів першорядним є встановлення власника, повідомлення та належне оформлення повернення.

Рішення про те, які матеріали є «необхідними», має дискреційний характер. Проблема виникає тоді, коли процедура не залишає хоча б мінімального сліду для перевірки: у такому разі вона стає непрозорою. У цифровому контексті ризик ще гостріший – навіть добросовісне рішення не гарантує, що всі копії та резерви будуть охоплені.

Раціональним компромісом виглядає перевірюваність за метаданими без розкриття чутливого змісту. У постанові про знищення та в акті знищення варто фіксувати: ідентифікатор об'єкта (тип, носій, часовий діапазон, технічні маркери), місця зберігання, відповідальних осіб, згадку про охоплення копій / резервів і спосіб контролю виконання. Так процедура стає надійнішою і менш вразливою до довільності, не відкриваючи приватний зміст [7–9]. З позиції справедливого суду та рівності сторін важливо, щоб знищення невикористаних матеріалів не перетворювалося на інструмент процесуальної непрозорості для захисту, а супроводжувалося перевірюваними процедурними слідами, достатніми для контролю без розкриття змісту [8].

Оперативність знищення має гарантійний сенс: що довше надлишкові матеріали залишаються доступними, то вищі ризики витоку або несанкціонованого використання [4]. Водночас у цифровому середовищі це не зводиться до одноразового «видалення». Дані можуть залишатися в робочих дублікатах, резервних копіях, логах доступу, синхронізованих сховищах і похідних матеріалах [5]. Тому практично виправданою є двоступенева модель:

– інвентаризація місць зберігання + тимчасове обмеження доступу;

– знищення / припинення доступу + акт, що підтверджує охоплення копій / резервів.

Норма «не використовувати» працює лише тоді, коли система робить непомітне копіювання або експорт складним і залишає фіксацію в журналах. Тому поряд із формальною забороною потрібні механізми, які забезпечують її виконуваність:

– рольовий доступ;

– логування перегляду та експорту;

– контроль зовнішніх носіїв і друку;

– аудит журналів;

– організаційні правила мінімізації копій [9].

Емпіричні дослідження надійності цифрових криміналістичних процесів підтверджують, що саме документованість, відтворюваність та контроль виконання стандартів є ключовими для оцінки надійності процедур, зокрема в роботі з цифровими носіями та копіями [9].

Повернення майна власнику в межах спеціального режиму скорочує період контролю державою і водночас захищає право власності. Доцільно оформлювати його актом приймання-передачі, де окремо зазначається: чи створювалися копії / образи (для цифрових носіїв), чи знищені вони і чи припинено доступ до них. Без такої фіксації легко виникає ситуація «носій повернули – цифрового двійника залишили».

Знищення матеріалів не скасовує процесуального обов'язку повідомлення осіб, щодо яких проводилися НСРД [4]. Отже, потрібен мінімальний облік, достатній для виконання цього обов'язку (метадані проведення та рішень), але без збереження надлишкового приватного змісту.

У підходах ЄСПЛ гарантії щодо негласного спостереження розглядаються як взаємопов'язана система: від підстав санкціонування до правил доступу, зберігання, використання й знищення [10; 12]. Аналіз справи Big Brother Watch підкреслює, що запобіжники оцінюються комплексно, і правила поводження з даними після їх отримання (включно зі знищенням надлишкових матеріалів та обмеженням вторинного використання) є визначальними для висновку про належність закону в розумінні практики ЄСПЛ [12]. З цього випливають орієнтири: процедура знищення має бути реальною (з урахуванням копій і резервів), контроль – ефективним, а перевірюваність – досяжною через метадані без розкриття змісту.

Мінімальні реквізити постанови прокурора про знищення: реквізити провадження; правова підстава; перелік об'єктів знищення з технічними маркерами (без змісту); місця зберігання; окремий блок про копії / резерви; відповідальні; строк виконання; спосіб контролю.

Уніфікований акт знищення цифрових даних: посилання на постанову; повторна ідентифікація об'єктів; спосіб знищення/припинення доступу; підтвердження охоплення копій / резервів; час операцій; підписи відповідальних; за можливості – контрольні ознаки (хеш) архіву до знищення.

Аудит доступу як стандарт: журналювання і періодичний аудит доступу, зокрема між рішенням про «необхідність» і фактичним знищенням. Формалізація повернення майна: акт приймання-передачі із зазначенням, чи створювалися копії та яка їхня доля.

Висновки. Спеціальний режим невикористаних матеріалів НСРД є гарантійним механізмом, що поєднує виведення надлишкових матеріалів з обігу, обмеження доступу і заборону вторинного використання, а також процедури повернення майна й повідомлення осіб [4].

У цифровому середовищі «знищення» доцільно тлумачити як доведений стан фактичної недоступності змісту та припинення обігу даних. Це потребує інвентаризації місць зберігання і контролю копій / резервів, адже множинність копій робить формальне «видалення» недостатнім [2; 5]. Водночас дослідження з безпечного видалення наголошують, що саме резервні контури, журнали та похідні артефакти є типово недооціненими «точками виживання» даних після видалення [2; 5].

Свобода ухвалення рішення прокурором щодо «необхідності» матеріалів має супроводжуватися мінімальною перевірюваністю без розкриття чутливого змісту. Стандартизована постанова і уніфікований акт знищення з технічними ідентифікаторами та блоком щодо копій / резервів знижують ризик довільності й підсилюють підзвітність [7–9].

Підходи ЄСПЛ підтверджують: правила доступу, зберігання, використання і знищення даних є елементом належності закону в розумінні практики ЄСПЛ та оцінки пропорційності втручання [10; 12].

Особистий внесок автора: обґрунтовано тлумачення «знищення» як фактичної недоступності змісту в цифровому середовищі; запропоновано модель мінімальної перевірюваності рішень прокурора через метадані без розкриття змісту; сформульовано практичні стандарти постанови про знищення, акта знищення цифрових даних та акта приймання-передачі при поверненні майна.

Перспективи подальших розвідок: розроблення типових форм документів (постанова / акт / акт передачі) та методики аудиту доступу до матеріалів НСРД з урахуванням різних архітектур зберігання (локальні сховища, відомчі системи, централізовані архіви, резервні контури).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : затв. наказом Генеральної прокуратури України, МВС України, СБУ, Адміністрації ДПСУ, Міністерства фінансів України, Міністерства юстиції України від 16.11.2012 № 114/1042/516/1199/936/1687/5 // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/v0114900-12#Text

2. Joukov, N., Papaxenopoulos, H., Zadok, E. Secure deletion myths, issues, and solutions // Proceedings of the Second ACM Workshop on Storage Security and Survivability (StorageSS). 2006. DOI 10.1145/1179559.1179571

3. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР (зі змін.). URL : https://zakon.rada.gov.ua/laws/show/254к/96-вр

4. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI (зі змін.). Ст. 253 «Повідомлення осіб, щодо яких проводилися негласні слідчі (розшукові) дії»; ст. 255 «Заходи щодо захисту інформації, яка не використовується у кримінальному провадженні». URL : https://zakon.rada.gov.ua/laws/show/4651-17

5. Reardon, J., Basin, D., Čapkun, S. SoK: Secure data deletion // 2013 IEEE Symposium on Security and Privacy. 2013. P. 301–315. DOI 10.1109/SP.2013.28

6. Sommardal, J. National security secrecy in ECtHR proceedings-the Court's eroding toolbox against unjustified secrecy and abuse. *Human Rights Law Review.* 2025. Vol. 25, Issue 3. Article ngaf024. DOI 10.1093/hrlr/ngaf024

7. Stoykova, R. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review.* 2021. Vol. 42. Article 105575. DOI 10.1016/j.clsr.2021.105575

8. Stoykova, R. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations. *Computer Law & Security Review.* 2023. Vol. 49. Article 105801. DOI 10.1016/j.clsr.2023.105801

9. Stoykova, R., Andersen, S., Franke, K., Axelsson, S. Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation.* 2022. Vol. 40. Article 301351. DOI 10.1016/j.fsidi.2022.301351

10. Turanjanin, V. When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights approach. *International Cybersecurity Law Review.* 2023. DOI 10.1365/s43439-022-00074-7

11. White, M. The Investigatory Powers Tribunal and bulk communications data acquisition: Lacking respect for the right to privacy and fundamental rights? *European Data Protection Law Review.* 2021. Vol. 7, Issue 1. P. 74–90. DOI 10.21552/edpl/2021/1/10

12. Zalnieriute, M. Big Brother Watch and Others v. the United Kingdom. *American Journal of International Law.* 2022. Vol. 116, Issue 3. P. 585–592. DOI 10.1017/ajil.2022.35

V. O. Romanov. UNUSED MATERIALS FROM COVERT INVESTIGATIVE (SEARCH) ACTIONS: REGIME, DESTRUCTION, AND CONTROL

Covert investigative (search) actions (CISA) involve concealed interference with private life. In such circumstances, the person affected has no real opportunity to immediately verify the lawfulness of the interference or to use procedural safeguards. Privacy protection therefore depends not only on whether CISA were properly authorised, but also on what happens to the materials afterwards: how they are selected, where and how they are stored, who can access them, whether reuse is possible, and under what procedures the data become genuinely inaccessible. A substantial share of information collected through CISA does not acquire evidentiary value or is not introduced into proceedings at all, yet it may continue to exist as a document, a physical item, a storage medium, or a digital copy.

In digital environments, the risk stems not only from retention but also from the data's ability to "reappear" through duplicates and technical traces-backups, access logs, synchronised repositories. Moreover, in many systems "deletion" is primarily a logical operation: the content may remain available in other storage layers or backup circuits. Destruction, therefore, should rest on verifiable procedures rather than a single technical step.

The purpose of this article is to clarify the substance of the special regime governing unused CISA materials, identify typical risks of its implementation under digitalisation, and propose practical solutions that strengthen accountability and make destruction effective in practice. The study applies a formal legal analysis of procedural rules on destruction, prohibitions on third-party access and use, the return of items/documents, and notification of persons; a systemic approach to privacy guarantees; and a functional analysis of organisational and technical control barriers (role-based access, logging, audit, and controls over copying and export). It also draws on the European Court of Human Rights' approach to the "quality of law" requirement and findings from research on secure data deletion and the reliability of digital evidence.

A working typology of unused CISA materials is proposed (records/attachments; storage media; items and documents; derivative materials), demonstrating that the special regime must cover the entire circulation of sensitive data rather than focusing narrowly on evidentiary status. In the digital context, "destruction" should be understood as a proven state of factual inaccessibility of content and the cessation of data circulation-something unattainable without an inventory of storage locations, accounting for copies and backups, and proper

documentation of execution. Likewise, prohibitions on third-party use are meaningful only when supported by control mechanisms: role separation, logging, auditing, and restrictions on copying and export.

As practical measures, the article proposes a minimum set of required elements for a prosecutor's destruction order (identification of objects without disclosing content; storage locations; a separate section on copies/backups; timeframe; responsible persons; and the method of oversight), a unified act for the destruction of digital data that records coverage of backups/synchronisations, and formalised return of property via an acceptance–transfer act that specifies the fate of copies. Regular audits of access to sensitive information are emphasised as a baseline standard of accountability.

Keywords: *covert investigative (search) actions, unused materials, information destruction, digital data, prosecutorial oversight, privacy, access audit, backups, role-based access, return of items.*

Дата надходження 11.02.2026
Дата прийняття 16.02.2026
Дата рекомендації 25.03.2026
Дата публікації 15.05.2026