

РЯБЧИНСЬКА О. П.,доктор юридичних наук, професор,
професор кафедри кримінального права
та правоохоронної діяльності*(Запорізький національний університет)*

ORCID ID: 0000-0002-9012-3332

Стаття поширюється на умовах ліцензії CC BY 4.0

УДК 342.721:343.2/.7:351.74

DOI <https://doi.org/10.32842/2078-3736/2025.4.2.43>**ТЕМПОРАЛЬНІ МЕЖІ ЗБЕРІГАННЯ ПЕРСОНАЛЬНИХ ДАНИХ
ПРАВООХОРОННИМИ ТА АНТИКОРУПЦІЙНИМИ ОРГАНАМИ:
ЗАГАЛЬНИЙ ТА СПЕЦІАЛЬНИЙ ЄВРОПЕЙСЬКІ СТАНДАРТИ**

Наукова стаття присвячена комплексному дослідженню правової природи та практичних аспектів встановлення темпоральних меж зберігання персональних даних у діяльності правоохоронних органів. Актуальність дослідження зумовлена потребою адаптації українського законодавства до вимог Директиви (ЄС) 2016/680 (LED) та практики ЄСПЛ у контексті забезпечення права на повагу до приватного життя (ст. 8 ЄКПЛ). Дослідження підтверджує, що нормативно-правове регулювання в Україні поступово наближається до європейських стандартів. Позитивним прикладом визначено функціонування ІП «Адмінпрактика», де впроваджено автоматичне знеособлення даних через один рік, що відповідає принципу обмеження строків зберігання. Автор доводить, що ефективність правоохоронних баз залежить від балансу між державним інтересом та приватністю: так, тривале зберігання інформації (15–25 років) у системах розшуку зниклих осіб є виправданим і відповідає позитивним обов'язкам держави за ст. 2 та ст. 8 ЄКПЛ. Водночас виявлено прогалини у веденні Реєстру корупціонерів. Головною проблемою є відсутність кореляції між кримінально-правовим інститутом погашення судимості та адміністративною процедурою виключення відомостей з електронного реєстру. Обґрунтовано, що відсутність чіткої процедури знищення даних у підзаконних актах розпорядника не може бути перешкодою для захисту прав особи. Оскільки норми ст. 59 ЗУ «Про запобігання корупції» є нормами прямої дії, вони мають пріоритет над відомчими обмеженнями. Звертається увага, що розпорядник (НАЗК) зобов'язаний видаляти застарілі відомості за ініціативним зверненням суб'єкта безпосередньо на підставі закону, адже відсутність внутрішнього регламенту не звільняє державний орган від обов'язку забезпечити приватність особи. У висновках наголошено на необхідності уніфікації підходів до всіх правоохоронних систем шляхом запровадження алгоритмічного видалення даних одразу після настання юридичного факту (спливу строків або погашення судимості). Такий підхід дозволить мінімізувати вплив «людського фактору» та забезпечити реальну відповідність принципам LED та ЄКПЛ, запобігаючи ризикам неправомірного втручання в приватне життя людини.

Ключові слова: *персональні дані, правоохоронні органи, темпоральні межі зберігання, Директива (ЄС) 2016/680 (LED), Стаття 8 ЄКПЛ, правоохоронні бази даних, Реєстр корупціонерів, законність, конфіденційна інформація, захист персональних даних.*



Riabchynska O. P. Temporal limits of personal data storage by law enforcement and anti-corruption agencies: general and special european standards

The scientific article is devoted to a comprehensive study of the legal nature and practical aspects of establishing temporal limits for the storage of personal data in the activities of law enforcement agencies. The relevance of the research is conditioned by the need to adapt Ukrainian legislation to the requirements of Directive (EU) 2016/680 (LED) and the case-law of the ECtHR in the context of ensuring the right to respect for private life (Article 8 of the ECHR). The study confirms that the regulatory framework in Ukraine is gradually aligning with European standards. A positive example is the functioning of the "Adminpraktika" information system, which has implemented automatic depersonalization of data after one year, consistent with the principle of storage limitation. The author argues that the effectiveness of law enforcement databases depends on maintaining a balance between the public interest and individual privacy: for instance, long-term data retention (15–25 years) in systems for missing persons and unidentified bodies is justified and corresponds to the state's positive obligations under Articles 2 and 8 of the ECHR. At the same time, gaps in the maintenance of the Register of Corrupt Persons have been identified. The main problem is the lack of correlation between the criminal law institute of expungement (clearing) of a criminal record and the administrative procedure for removing information from the electronic register. It is substantiated that the absence of a clear data destruction procedure in the administrator's bylaws cannot be an obstacle to protecting an individual's rights. Since the provisions of Article 59 of the Law of Ukraine "On Prevention of Corruption" are norms of direct effect, they take priority over departmental restrictions. Attention is drawn to the fact that the administrator (NAZK) is obliged to delete outdated information upon the initiative of the data subject directly on the basis of the law, as the lack of an internal regulation does not exempt a state body from the obligation to ensure the privacy of an individual. The conclusions emphasize the need to unify approaches to all law enforcement systems by introducing an algorithmic data deletion mechanism immediately upon the occurrence of a legal fact (expiration of terms or expungement of a criminal record). Such an approach will minimize the influence of the 'human factor' and ensure real compliance with the LED and ECHR principles, preventing the risks of unlawful interference with an individual's private life.

Key words: *personal data, law enforcement agencies, temporal limits of storage, Directive (EU) 2016/680 (LED), Article 8 ECHR, law enforcement databases, Register of Corrupt Persons, legality, confidential information, personal data protection.*

Постановка проблеми. У сучасному цифровому світі персональними даними особи розпоряджаються різноманітні суб'єкти владних повноважень. Інтенсивна цифрова трансформація зумовила системне накопичення відомостей про приватне життя у реєстрах різних відомств: від базових ідентифікаційних даних та метаданих електронних комунікацій до найбільш чутливих персональних даних, зокрема біометричних параметрів і генетичних профілів особи. Такий стан речей пов'язаний передусім із тим, що правоохоронні органи, виконуючи безпекові функції, наділені спеціальною правосуб'єктністю у сфері збору даних, як от проведення негласних розшукових заходів, ведення біометричних обліків та здійснення заходів із зняття інформації з транспортних телекомунікаційних мереж. Водночас, згідно зі статтею 8 Конвенції про захист прав людини і основоположних свобод (далі ЄКПЛ), реалізація цієї правосуб'єктності суворо обмежена: будь-яке втручання у приватність, зокрема через тривале зберігання інформації, має бути не лише законним, а й «необхідним у демократичному суспільстві», тобто пропорційним переслідуваній меті [1]. Відтак, невідповідність процесів зберігання даних критеріям «законності» та «необхідності» може бути підставою для оцінки дій правоохоронних органів як протиправних. Саме тому першочергового



значення набуває чітке визначення підстав та темпоральних меж законного зберігання інформації, оскільки будь-яке утримання персональних даних поза межами визначеного законом строку трансформує легітимний захід у протиправне втручання. При цьому основний акцент робиться саме на діяльності суб'єктів владних повноважень, а не приватних осіб. Це зумовлено специфікою їхнього правового статусу, оскільки згідно зі ст. 19 Конституції України, такі суб'єкти зобов'язані діяти лише на підставі, в межах та у спосіб, що передбачені Конституцією та законами України [2].

Аналіз останніх досліджень і публікацій. Питанням правового регулювання інформаційних відносин та захисту персональних даних присвячені численні публікації фахівців в сфері інформаційного права, адміністративного, конституційного та міжнародного права (П.М. Рабіновича, М. В. Савчина, С. В. Шевчука та ін.). Актуальні питання дотримання невтручання в приватне життя особи під час проведення негласних слідчих розшукових дій аналізувалися спеціалістами з кримінального процесуального права (І. В. Басистою, М. В. Бемом, І. В. Гловюк, О. В. Капліною, О. О. Торбасом, О. Г. Шило та ін.). Кримінально-правова охорона приватного життя людини, зокрема щодо невтручання шляхом збору та збереження персональних даних особи, досліджувалася С.Я. Лиховою, Ю.І. Демяненко, О.П. Горпинюк, О.В. Сосніною, Е.Г. Стоматовим та ін. Попри значний доробок зазначених науковців, питання темпоральних меж законного зберігання персональних даних правоохоронними органами в умовах стрімкої цифровізації залишається недостатньо з'ясованим. Зокрема, потребує додаткового аналізу момент трансформації легітимного утримання конфіденційної інформації в базах даних (реєстрах) у протиправне втручання в приватне життя особи, що зумовлює необхідність встановлення чітких критеріїв такої діяльності у контексті стандартів «законності» та «необхідності у демократичному суспільстві».

Метою статті є встановлення критеріїв відповідності процедур зберігання персональних даних у правоохоронній сфері принципам «законності» та «необхідності в демократичному суспільстві», а також виявлення правових ризиків, що виникають унаслідок недотримання темпоральних меж розпорядження такою інформацією.

Виклад основного матеріалу. Так, в ч. 4 ст. 31 Закону України «Про інформацію» встановлене загальне правило, що зберігання інформації про громадян не повинно тривати довше, ніж це необхідно для встановленої законом мети [3]. Відповідно до Закону України «Про захист персональних даних» останні підлягають видаленню або знищенню у разі: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних [4].

Відповідно до ч.12 ст. 9 Закону України «Про оперативно-розшукову діяльність» одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій, зберігання не підлягають і повинні бути знищені. Порядок знищення таких відомостей визначено в «Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» [5]. Відповідно до абз. 2 ч. 3 ст. 22 Закону України «Про організаційно-правові основи боротьби зі злочинністю» документи та інші джерела, що містять таку інформацію, підлягають знищенню не пізніше шести місяців з дня їх одержання відповідним спеціальним органом по боротьбі з організованою злочинністю [6].

Відповідно до Порядку обробки та захисту отриманих від суб'єктів надання інформації персональних даних під час здійснення перевірки достовірності інформації та документів, що внесені до електронної системи охорони здоров'я (крім інформації про стан здоров'я людини), на підставі яких формуються звіти, що є підставою для оплати наданих медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій, або які



містять персональні дані пацієнтів, медичних працівників, яким (якими) надано відповідні медичні послуги, лікарські засоби та медичні вироби персональні дані в інформаційно-аналітичній платформі зберігаються протягом строку, необхідного для цілей перевірки достовірності інформації та документів, але не довше 5 років [7].

Отже знищення персональних даних (певної конфіденційної інформації) особи обумовлено такими факторами: 1) закінчення визначеного згодою суб'єкта персональних даних строку обробки таких даних; 2) закінчення визначеного законом строку зберігання таких даних (6 місяців, 5 років тощо); 3) настанням певного юридичного факту (дії, події тощо), як от припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником таких даних, видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого чи набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

Виходячи з того, що знищення конфіденційної інформації щодо особи, яка збиралася та зберігалася на законних підставах, є частиною встановленого законом порядку поводження з такою інформацією, відтак її не знищення чи знищення не у визначений строк може розглядатися як порушення такого порядку та утворювати незаконне зберігання у разі вчинення таких дій умисно.

Положення законів щодо строковості збереження персональних даних базуються на вимогах GDPR, відповідно до яких персональні дані не можуть зберігатися довше, ніж це необхідно для цілей, для яких здійснюється обробка персональних даних (стаття 5(1)(c) і (e) GDPR). У деяких державах-членах можуть існувати окремі положення щодо термінів зберігання даних відеоспостереження відповідно до статті 6 (2) GDPR. Контролер несе відповідальність за визначення періоду зберігання таких записів відповідно до принципів необхідності та пропорційності, а також за доведення відповідності положенням GDPR [8].

Утім варто урахувати, що GDPR є загальним стандартом (*lex generalis*), тоді як спеціальним стандартом (*lex specialis*) для суб'єктів правоохоронної діяльності визнається Директива (ЄС) 2016/680 Європейського парламенту і ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних компетентними органами для цілей запобігання, розслідування, виявлення або судового переслідування кримінальних правопорушень або виконання кримінальних покарань, і про вільний рух таких даних, та про скасування Рамкового рішення Ради 2008/977/ПВД (далі – LED) [9]. Зокрема в ст. 5 якої вказано, що Держави-члени повинні передбачити встановлення відповідних граничних строків для видалення персональних даних або для періодичного перегляду потреби у зберіганні персональних даних. Процесуальні заходи повинні забезпечувати дотримання цих граничних строків. Хоча станом на сьогодні вказані акти не мають прямої дії на території України, держава має імплементувати їхні положення в національне законодавство на виконання міжнародно-правових зобов'язань відповідно до Угоди про асоціацію між Україною та ЄС.

В Типовому порядку обробки персональних даних, затвердженому Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14 (далі – Типовий порядок) [10] серед вимог до обробки персональних даних передбачено, що володілець визначає мету та підстави обробки персональних даних, а також порядок їх обробки. Серед іншого – строк та умови зберігання таких даних, умови та процедуру їх зміни, видалення або знищення. Персональні дані обробляються у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, у строк не більше, ніж це необхідно відповідно до мети їх обробки (п. 2.10 Типового порядку). Важливим положенням є те, що у разі зміни визначеної мети обробки персональних даних на нову мету, яка є несумісною з попередньою, для подальшої обробки даних володілець персональних даних, окрім випадків, визначених законодавством, повинен отримати згоду суб'єкта персональних даних на обробку його даних відповідно до нової мети.

Зберігання є частиною процесу обробки персональних даних персонал будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача),



знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем (ст. 2 ЗУ «Про захист персональних даних») [4]. Відтак підстави для обробки даних повною мірою поширюються й на зберігання персональних даних. Обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли така згода не вимагається Законом.

До випадків, коли персональні дані обробляються (зокрема й зберігаються) без згоди суб'єкта персональних даних закон відносе наступні:

1) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (сфера надання державних послуг, сфера соціального захисту, військовий облік, фінансовий моніторинг, охорона здоров'я, правоохоронна діяльність та правосуддя тощо);

2) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних (у випадках надання банківських послуг (відкриття рахунку), комунальні послуги, страхування життя/здоров'я роботодавцем та ін.);

3) захист життєво важливих інтересів суб'єкта персональних даних (у випадках екстреної медичної допомоги, у разі надзвичайних ситуацій та катастроф, запобігання кримінальним правопорушенням та ін.);

4) необхідність виконання обов'язку володільця персональних даних, який передбачений законом (ключовими сферами є податкова звітність, фінансовий моніторинг, військовий облік на підприємстві, державна реєстрація прав власності та ін.);

5) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси (ст. 11 ЗУ «Про захист персональних даних») (захист майна, безпекові заходи (відеоспостереження), запобігання шахрайству, прямий маркетинг та ін.).

Отже, діяльність правоохоронних органів ґрунтується на підставах обробки даних без згоди особи, позаяк їх функціонування є прямою реалізацією державних функцій та обов'язків, визначених законодавством. Ключовими сферами є: здійснення повноважень володільця персональних даних (п. 5 ч. 1 ст. 11 ЗУ «Про захист персональних даних») та захист життєво важливих інтересів (п. 4 ч. 1 ст. 11 цього Закону). Водночас, навіть за таких умов, правоохоронні органи як володільці зобов'язані використовувати дані виключно для законної мети, дотримуватися принципу адекватності (мінімізація збору) та забезпечувати їх видалення після виконання повноважень. Вони суворо обмежені принципом законності, що передбачає обов'язкову фіксацію кожного звернення до реєстрів для запобігання зловживанням (аудит) та отримання судового дозволу на найбільш суттєві втручання в приватність у процесі проведення негласних слідчих (розшукових) дій: доступу до змісту приватного листування в месенджерах, отримання метаданих і записів телефонних розмов, контролю за поштовими відправленнями, а також зняття інформації з електронних комунікаційних мереж та інших технічних засобів.

Відповідно до Закону України «Про захист персональних даних» [4] останні підлягають видаленню або знищенню у разі: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2) припинення правовідносин між суб'єктом персональних даних та володільцем чи розпорядником, якщо інше не передбачено законом; 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

Тож строк зберігання персональних даних особи може визначатися: 1) в згоді на обробку персональних даних; 2) в профільному законі (чи іншому нормативно-правовому акті), що визначає підстави та порядок отримання, зберігання та знищення персональних



даних особи (конфіденційної інформації) – без (або незалежно від згоди суб'єкта персональних даних) у всіх інших випадках, передбачених ч. 1 ст. 11 Закону України «Про захист персональних даних».

Для правоохоронних органів (СБУ, Національної поліції, НАБУ тощо) ці терміни деталізуються у спеціальних законах, Кримінальному процесуальному кодексі та відомчих нормативних актах, які встановлюють межі зберігання відомостей у реєстрах, матеріалах справ та оперативних базах даних залежно від мети їх збору.

Зокрема, в ч. 12 ст. 9 Закону України «Про оперативно-розшукову діяльність» одержані внаслідок оперативно-розшукової діяльності відомості, що стосуються особистого життя, честі, гідності людини, якщо вони не містять інформації про вчинення заборонених законом дій, зберігання не підлягають і повинні бути знищені. Порядок знищення таких відомостей визначено в «Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні» [5].

Відповідно до абз. 2 ч.3 ст. 22 ЗУ «Про організаційно-правові основи боротьби зі злочинністю» документи та інші джерела, що містять таку інформацію, підлягають знищенню не пізніше шести місяців з дня їх одержання відповідним спеціальним органом по боротьбі з організованою злочинністю [6].

В Інструкції з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції передбачено, що порядок збирання, обробки, накопичення, зберігання персональних даних і доступ до них здійснюється відповідно до Законів України «Про захист інформації в інформаційно-комунікативних системах» та «Про захист персональних даних» (п. 7 Розділу III цієї інструкції) [11].

В Інструкції з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» передбачено, що інформація в базі даних «Розшук» зберігається впродовж п'ятнадцяти років з дня закриття оперативно-розшукової справи «Розшук» або розшукової справи, крім: 1) осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від відбування покарання або від виконання обов'язків, визначених законом для суб'єктів пробації, стосовно яких застосовується положення щодо строків давності, визначені частинами четвертої та п'ятої статті 49 Кримінального кодексу України, а також осіб, зниклих безвісти, зокрема за особливих обставин та невідомих трупів – тіла (останки) осіб, персональні дані яких на момент виявлення невідомі та встановлення яких потребує проведення пошукових заходів інформація щодо яких зберігається впродовж двадцяти п'яти років з дня закриття ОРС «Розшук» або РС; 2) дітей, стосовно яких за виконавчим документом про відібрання дитини за поданням виконавця судом винесено ухвалу про їх розшук, інформація щодо яких зберігається до досягнення ними повноліття [12].

В Інструкції з формування та ведення інформаційної підсистеми «Адміністративна практика» інформаційно-комунікативної системи «Інформаційний портал Національної поліції України» передбачено, що інформація про особу, внесена до цієї інформаційної підсистеми (прізвище, власне ім'я, по батькові (за наявності) особи, яка вчинила адміністративне правопорушення, дата і місце його народження, місце проживання (перебування) (країна, область, район, населений пункт, вулиця, номер будинку, корпус, квартири); документ, що посвідчує особу, вилучається шляхом їх видалення, що виключає подальшу можливість поновлення таких відомостей. Процес знеособлення відбувається одразу після зняття з автоматизованого обліку через рік із дати вчинення адміністративного правопорушення (Розділ IV Інструкції) [13].

В обох інструкціях передбачено, що знеособлення відомостей (персональних даних) здійснюється шляхом їх видалення, що виключає подальшу можливість поновлення таких відомостей. Водночас в Інструкції щодо ІП «Адмінпрактика» системи ІПНП, чітко зазначається, що зняття з обліку відомості знеособлюються автоматично. І це в більшій мірі відповідає вимогам Директиви ЄС 2016/680 (LED).



Строки зберігання відомостей в Єдиному державному реєстрі осіб, які вчинили корупційні або пов'язані з корупцією кримінальні правопорушення визначені безпосередньо у Законі України «Про запобігання корупції». Так, у ч. 4 ст. 59 цього Закону (якою її було доповнено на підставі Закону України № 4496-IX від 17 червня 2025 року [14]) передбачено такі строки: 1) один рік для відомостей про притягнення до цивільно-правової відповідальності фізичної особи за вчинення корупційних або пов'язаних з корупцією правопорушень; 2) один рік – для відомостей про накладення адміністративного стягнення на фізичну особу за вчинення корупційного або пов'язаного з корупцією правопорушення; 3) до погашення або зняття судимості з особи – для відомостей про притягнення до кримінальної відповідальності фізичної особи за вчинення корупційних або пов'язаних з корупцією правопорушень – до погашення або зняття судимості з особи; 4) п'ять років для відомостей про юридичних осіб, до яких застосовано заходи кримінально-правового характеру у зв'язку з вчиненням корупційного правопорушення [15].

Після закінчення строків, визначених цією частиною, відомості про особу в Єдиному державному реєстрі осіб, які вчинили корупційні або пов'язані з корупцією правопорушення, підлягають виключенню.

Звертає увагу той факт, що закон зобов'язує видалити такі відомості, але Положення про державний реєстр осіб, які вчинили корупційні або пов'язані з корупцією правопорушення не містить чіткої процедури яким чином це має бути здійснено саме у випадку сплину строків погашення чи знання судимості з особи, яка була засуджена за таке діяння. Мова йде про те, що в згаданому положенні передбачені вичерпні підстави вилучення з Реєстру відомостей про особу, яка вчинила корупційне або пов'язане з корупцією правопорушення. Такими підставами є: 1) ухвала суду про скасування вироку; 2) винесення виправдувального вироку; 3) відновлення пропущеного строку на апеляційне оскарження; 4) скасування постанови про накладення адміністративного стягнення за корупційне або пов'язане з корупцією правопорушення; 5) розпорядчий документ або судові рішення про скасування розпорядчого документа про накладення дисциплінарного стягнення; 6) заява особи, яка з 24 лютого 2022 року до припинення або скасування воєнного стану брала безпосередню участь у заходах, необхідних для забезпечення оборони України, захисту безпеки населення та інтересів держави, у зв'язку з військовою агресією Російської Федерації проти України у складі Збройних Сил України, Державної прикордонної служби України, Державної спеціальної служби транспорту, Державної служби спеціального зв'язку та захисту інформації України, Національної гвардії України, Служби безпеки України, Служби зовнішньої розвідки України, Управління державної охорони України, інших утворених відповідно до законів України військових формувань.

Отже, наявна нормативна колізія, за якої імперативна вимога ЗУ «Про запобігання корупції» щодо виключення відомостей з реєстру після погашення судимості не підкріплена відповідним механізмом у Положенні про Реєстр. Оскільки перелік підстав для вилучення даних є вичерпним і включає лише скасування рішень або спеціальні умови для військових, у системі виникає процедурна прогалина, суть якої полягає у тому, що автоматичне погашення судимості за законом фактично ігнорується реєстратором через відсутність такої підстави в інструкції. Така ситуація йде в розріз усталеною практикою ЄСПЛ (Справа «S. and Marper v. the United Kingdom» 2008 року [16]).

Тож встановлення чітких строків зберігання персональних даних у цьому реєстрі є кроком до імплементації принципів LED, проте проблема їхньої автоматичної реалізації в реєстрах залишається відкритою. Відсутність у Положенні про Реєстр механізму автоматичного очищення бази даних після погашення судимості перетворює правоохоронний облік на безстроковий захід впливу. Це свідчить, з одного боку, про незавершеність імплементації окремих цільових стандартів LED щодо чіткого алгоритму видалення персональних даних за наявності для того правових підстав, а з іншого – про неналежне виконання позитивного обов'язку за ст. 8 Європейської конвенції. За логікою ЄСПЛ, таке інертне зберігання інформації є непропорційним втручанням у права особи та формою незаконної обробки персональних даних.



Виходом із ситуації є письмове звернення до НАЗК із вимогою про виключення відомостей, що ґрунтується на прямій дії норми Закону України «Про запобігання корупції» (ст. 59). Оскільки Закон має вищу юридичну силу, ніж Положення, реєстратор зобов'язаний видалити дані після закінчення строків зберігання (погашення судимості), навіть за відсутності такої процедури в інструкції. Таке звернення долає нормативну прогалину та змушує адміністратора Реєстру забезпечити ваше право «бути забутим» на підставі імперативної вимоги закону. Такий порядок ґрунтується на загальних нормах законів України. Зокрема, в ст. 10 Закону України «Про доступ до публічної інформації» кожній особі гарантується зокрема право вимагати виправлення неточної, неповної, застарілої інформації про себе, знищення інформації про себе, збирання, використання чи зберігання якої здійснюється з порушенням вимог закону [17], а в ЗУ «Про захист персональних даних» прямо передбачено, що персональні дані підлягають виділенню у разі закінчення строку їх зберігання (ст. 15) [4].

Висновки. Дослідження підтверджує, що нормативно-правове регулювання ведення реєстрів та зберігання персональних даних у правоохоронних органах України поступово адаптується до вимог Директиви LED та практики ЄСПЛ щодо дотримання права на повагу до приватного життя (ст. 8 ЄКПЛ). Найбільш успішним прикладом є впровадження автоматичного знеособлення даних в ІП «Адмінпрактика» через один рік, що відповідає принципам пропорційності та обмеження строків зберігання інформації. Ефективність інших проаналізованих правоохоронних баз даних залежить від дотримання балансу між державним інтересом та приватністю особи, де тривалі строки зберігання інформації (15–25 років) у системах розшуку зниклих осіб та невпізнаних тіл є цілком виправданими та відповідають позитивним зобов'язанням держави за ст. 2 та ст. 8 ЄКПЛ.

Відсутність процедури знищення даних у підзаконних актах розпорядника не може бути перешкодою для реалізації прав особи, оскільки норми ст. 59 ЗУ «Про запобігання корупції» та профільного законодавства про захист персональних даних є нормами прямої дії, що мають пріоритет над відомчими обмеженнями. У такому разі правовим інструментом подолання прогалини стає ініціативне звернення суб'єкта з вимогою про видалення застарілих відомостей: розпорядник (НАЗК) зобов'язаний вчинити відповідні дії безпосередньо на підставі закону, оскільки відсутність внутрішнього регламенту не звільняє державний орган від обов'язку забезпечити право особи на захист її приватного життя. Для забезпечення реальної відповідності LED та ЄКПЛ, необхідно уніфікувати підхід до всіх правоохоронних систем, запровадивши механізм автоматичного (алгоритмічного) видалення персональних даних одразу після настання юридичного факту (спливу строків або погашення судимості), мінімізуючи вплив «людського фактору» та недосконалість відомчих інструкцій.

Список використаних джерел:

1. Конвенція про захист прав і основоположних свобод людини 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 10.08.2025).
2. Конституція України Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
3. Про інформацію : Закон України № 2657–ХІІ від 2 жовтня 1992 р. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
4. Про захист персональних даних : Закон України від 1 червня 2010 року № 2297–VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
5. Інструкція про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, затверджена Наказом Генеральної прокуратури України, Міністерства внутрішніх справ України, Служби безпеки України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України 16.11.2012 № 114/1042/516/1199/936/1687/5. URL: <https://zakon.rada.gov.ua/laws/show/v0114900-12/conv/parapp4.13:rz4#n113> (дата звернення 15.08.2025).



6. Про організаційно-правові основи боротьби зі злочинністю: Закон України від 30 червня 1993 року № 3341-XII. URL: <https://zakon.rada.gov.ua/laws/show/3341-12#Text> (дата звернення 15.08.2025).

7. Порядок обробки та захисту отриманих від суб'єктів надання інформації персональних даних під час здійснення перевірки достовірності інформації та документів, що внесені до електронної системи охорони здоров'я (крім інформації про стан здоров'я людини), на підставі яких формуються звіти, що є підставою для оплати наданих медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій, або які містять персональні дані пацієнтів, медичних працівників, яким (якими) надано відповідні медичні послуги, лікарські засоби та медичні вироби. Затверджений Наказом міністерства фінансів України 01 травня 2024 року № 219. URL: <https://zakon.rada.gov.ua/laws/show/z0712-24#Text> (дата звернення 15.08.2025).

8. Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (дата звернення 15.08.2025).

9. Directive (EU) 2016/680 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. URL: <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng> (дата звернення 15.08.2025).

10. Типовий порядок обробки персональних даних, затверджений Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 р. № 1/02-14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (дата звернення 15.08.2025).

11. Інструкція з організації реагування на заяви і повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції, затверджена Наказом міністерства внутрішніх справ України 27 квітня 2020 року № 357. URL: https://zakon.rada.gov.ua/laws/show/z0443-20?find=1&text=зберігання+#w1_2 (дата звернення 15.08.2025).

12. Інструкція з формування та ведення бази даних «Розшук» інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України», затверджена Наказом Міністерства внутрішніх справ 28 червня 2023 року № 534. URL: https://zakon.rada.gov.ua/laws/show/z1486-23?find=1&text=зберігання+#w1_5 (дата звернення 15.08.2025).

13. Інструкція з формування та ведення інформаційної підсистеми «Адміністративна практика» інформаційно-комунікативної системи «Інформаційний портал Національної поліції України», затверджена Наказом Міністерства внутрішніх справ України від 13 березня 2023 року № 180. https://zakon.rada.gov.ua/laws/show/z0727-23?find=1&text=зберігання+#w1_1 (дата звернення 15.08.2025).

14. Про внесення змін до Кодексу України про адміністративні правопорушення, Кримінального кодексу України, Кримінального процесуального кодексу України та інших законодавчих актів України щодо підвищення відповідальності за корупційні або пов'язані з корупцією правопорушення»: Закон України від 17 червня 2025 року № 4496-IX. URL: <https://zakon.rada.gov.ua/laws/show/4496-20#n37> (дата звернення 15.08.2025).

15. Про запобігання корупції: Закон України від 14 жовтня 2014 року № 1700-VII. URL: <https://zakon.rada.gov.ua/laws/show/1700-18/sp:dark#Text> (дата звернення 15.08.2025).

16. SPABA S. AND MARPER v. THE UNITED KINGDOM. URL: <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-117631%22%5D%7D> (дата звернення 15.08.2025).

17. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення 15.08.2025).

Дата першого надходження рукопису до видання: 23.07.2025

Дата прийнятого до друку рукопису після рецензування: 23.08.2025

Дата публікації: 26.09.2025

