DOI: 10.33498/louu-2026-03-155



Наталія Ахтирська

кандидатка юридичних наук, доцентка,
начальниця Навчальної лабораторії
з вивчення права Європейського Союзу
Національної школи суддів України
(Київ, Україна)
ORCID ID: https://orcid.org/0000-0003-3357-7722
Researcher-ID 57222308510
Akhtyrska.n@gmail.com



Богдан Остудімов

PhD, головний науковий співробітник
Навчальної лабораторії
з вивчення права Європейського Союзу
Національної школи суддів України
(Київ, Україна)
markys78@ukr.net

УДК 343.1

ОБМЕЖЕННЯ ГАРАНТІЙ КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ У НАДЗВИЧАЙНИХ СИТУАЦІЯХ І ПІД ЧАС ВОЄННОГО СТАНУ: ПРАВО ЄС ТА ДОСВІД США

Анотація. Міжнародні стандарти гарантування та забезпечення прав людини формуються на основі презумпції одностайного розуміння цінності верховенства права та можливого застосування у разі конфлікту інтересів регламентованого порядку врегулювання дисбалансу. Особливий виклик виникає під час воєнного конфлікту, коли питання національної безпеки стають першочерговими.

Як свідчить історичний досвід, під час війни ворожа сторона використовує методи підриву державності, залякування населення, створення уявлення про неспроможність правоохоронних органів здійснювати заходи запобігання та протидії злочинності, ефективно проводити розслідування, а судами ухвалювати правосудні вироки. Для цього вдаються до терористичних загроз та інших дій, маючи на меті серйозно дестабілізувати чи зруйнувати основні політичні, конституційні, економічні або соціальні структури країни.

За даними Офісу Генерального прокурора, у 2025 р. було зареєстровано 608 101 кримінальне правопорушення, з яких особливо тяжких злочинів – 154 093, тяжких – 304 667. В умовах воєнного стану особливу загрозу становлять злочини проти основ національної безпеки України (5404), злочини проти громадської безпеки (8989) та ін. В Україні у 2025 р. виявлено 1070 випадків державної зради (ст. 111 Кримінального кодексу України, далі – КК

© Наталія Ахтирська, Богдан Остудімов, 2026

України), 1714 колабораційної діяльності, зареєстровано 160 кримінальних правопорушень за ст. 258 КК України "Терористичний акт" тощо. Водночас кількість кримінальних проваджень, за якими справи передані до суду, є значно меншими (з 608 101 провадження передано до суду з обвинувальним актом 139 707), що свідчить про певні процесуальні перешкоди в зборі доказів. Законодавцем внесені зміни до процесуального законодавства, які врахували особливості досудового розслідування в умовах воєнного стану, водночас тривалість бойових дій сформувала додаткові ризики та виклики, зокрема в тилу, шляхом вчинення вибухів під час транспортування поштових відправлень, використання sim-карт українців для використання в розвідувальних цілях тощо. Воєнний стан та інший надзвичайний стан, за досвідом інших держав, дає підстави законодавцю впровадити пропорційні загрозам механізми забезпечення безпеки держави.

Ключові слова: персональні дані; обмеження конфіденційності; воєнний стан; розширений доступ до даних за колом осіб без ухвали слідчого судді.

Міжнародні стандарти гарантування та забезпечення прав людини формуються на основі презумпції одностайного розуміння цінності верховенства права та можливого застосування у разі конфлікту інтересів регламентованого порядку врегулювання дисбалансу. Особливий виклик виникає під час воєнного конфлікту, коли питання національної безпеки стають першочерговими.

Як свідчить історичний досвід, під час війни ворожа сторона використовує методи підриву державності, залякування населення, створення уявлення про неспроможність правоохоронних органів здійснювати заходи запобігання та протидії злочинності, ефективно проводити розслідування, а судами ухвалювати правосудні вироки. Для цього вдаються до терористичних загроз та інших дій, маючи за мету серйозно дестабілізувати чи зруйнувати основні політичні, конституційні, економічні або соціальні структури країни.

За даними Офісу Генерального прокурора, у 2025 р. було зареєстровано 608 101 кримінальне правопорушення, з яких особливо тяжких злочинів – 154 093, тяжких – 304 667. В умовах воєнного стану особливу загрозу становлять злочини проти основ національної безпеки України (5404), злочини проти громадської безпеки (8989) та ін. В Україні у 2025 р. виявлено 1070 випадків державної зради (ст. 111 Кримінального кодексу України[1], далі – КК України), 1714 колабораційної діяльності, зареєстровано 160 кримінальних правопорушень за ст. 258 КК України "Терористичний акт" тощо. Водночас кількість кримінальних проваджень, за якими справи передані до суду, є значно меншими (з 608 101 провадження передано до суду з обвинувальним актом 139 707)[2], що свідчить про певні процесуальні перешкоди у зборі доказів. Законодавцем внесені зміни до процесуального законодавства, які врахували особливості досудового розслідування в умовах воєнно-

[1] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення 27.03.2026).

[2] Єдиний звіт про кримінальні правопорушення (січень–грудень 2025 р.). Офіс Генерального прокурора. <https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2> (дата звернення 27.03.2026).

го стану, водночас тривалість бойових дій сформувала додаткові ризики та виклики, зокрема в тилу, шляхом вчинення вибухів під час транспортування поштових відправлень, використання sim-карт українців для використання в розвідувальних цілях тощо. Воєнний стан та інший надзвичайний стан, за досвідом інших держав, дає підстави законодавцю впровадити пропорційні загрозам механізми забезпечення безпеки держави.

Виклики під час воєнного стану, коли неминуче посилюються загрози для безпеки держави, об'єктивно вимагають посилення безпеки, розвідки (внутрішньої / зовнішньої), кіберзахисту та боротьби з тероризмом, часто за участю правоохоронних органів, щоб протидіяти зривам і прямим атакам в умовах хаосу та потенційного зриву нормальних соціальних систем.

Угодою про асоціацію України з Європейським Союзом[3] передбачено обов'язок сторін співробітничати у боротьбі з кримінальною та незаконною організованою чи іншою діяльністю, а також з метою запобігання їй. Задля досягнення мети вважається за доцільне здійснювати обмін найкращими практиками, зокрема щодо методик розслідування та криміналістичних досліджень, обміну інформацією відповідно до існуючих правил.

Указом Президента України від 26 серпня 2021 р. затверджена Стратегія кібербезпеки України та введено в дію рішення Ради національної безпеки і оборони України від 14 травня 2021 р. "Про Стратегію кібербезпеки України"[4]. Ухвалення такого рішення зумовлено тим, що швидко змінюваний цифровий світ потребує формування більш збалансованої та ефективної національної системи кібербезпеки, яка *зможе гнучко адаптуватися до змін безпекового середовища.* Україна має забезпечити досягнення балансу між потребами суспільства, вітчизняного ринку, економіки держави та необхідними заходами з кібербезпеки, а також надійність і безпеку цифрових послуг протягом усього їхнього життєвого циклу. Україна має посилити спроможності у протидії кіберзлочинності шляхом: *завершення імплементації в законодавство України положень Конвенції про кіберзлочинність*[5]*; врегулювання на законодавчому рівні питання щодо електронних доказів, використовуючи кращі практики з цих питань Сполучених Штатів Америки, держав – членів ЄС.*

Варто зазначити, що право Європейського Союзу передбачає можливість *обмеження гарантій конфіденційності персональних даних у надзвичайних ситуаціях.* Європейський Союз створив мережу інструментів для захисту своїх громадян від терористичної загрози. Прихована, але безперервна боротьба ведеться на постійній основі та охоплює всі сфери. Хоча політика

[3] Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27.06.2014. <https://zakon.rada.gov.ua/laws/show/984_011#Text> (дата звернення 27.03.2026).

[4] Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 р. № 447/2021 <https://zakon.rada.gov.ua/laws/show/447/2021#n12> (дата звернення 27.03.2026).

[5] Конвенція про кіберзлочинність від 23.11.2001 <https://zakon.rada.gov.ua/laws/show/994_575#Text> (дата звернення 27.03.2026).

боротьби з загрозами залишається передусім національною компетенцією, європейська правова база дає змогу ЄС координувати засоби діяльності уповноважених органів у цій сфері.

Перше європейське антитерористичне співробітництво, спочатку неофіційне, було розпочато в 1975 р. Зіткнувшись зі зростаючою терористичною загрозою в Європі, європейські міністри з дев'яти держав – засновниць та асоційованих держав регулярно зустрічалися в рамках групи під назвою Trevi (Terrorism, Radicalism, Extremism and International Violence). Попри визнання та врегулювання питань захисту персональних даних, у Європейському Союзі з урахуванням загроз безпеці створено правову базу для збалансування дотримання верховенства права та суспільної безпеки. Завдання щодо питань запобігання та протидії злочинності, зокрема терористичній загрозі, потребували сучасних методів діяльності відповідних органів, зокрема оперативного доступу до персональних даних.

Директива про електронну приватність – Директива 2002/58/ЄС Європейського Парламенту та Ради від 12 липня 2002 р. щодо обробки персональних даних і захисту приватного життя в секторі електронних комунікацій – передбачає, що *держави-члени можуть обмежувати права громадян, якщо таке обмеження є необхідним, відповідним і пропорційним заходом у демократичному суспільстві для забезпечення національної безпеки, оборони, громадської безпеки або запобігання, розслідування, виявлення та переслідування кримінальних злочинів чи несанкціонованого використання системи електронних комунікацій.* Зокрема, у Директиві зазначено:

> Держави-члени можуть передбачити обмеження права користувача або абонента на приватність щодо ідентифікації лінії, з якої здійснюється дзвінок, коли це необхідно для визначення походження зловмисних дзвінків, а також щодо даних про ідентифікацію та місцезнаходження лінії, з якої здійснюється дзвінок, коли це необхідно для забезпечення максимально ефективного реагування служб екстреної допомоги. З цією метою держави-члени можуть прийняти спеціальні заходи, що дають змогу постачальникам електронних комунікаційних послуг надавати дані про ідентифікацію та місцезнаходження лінії, з якої здійснюється дзвінок, без попередньої згоди відповідного користувача або абонента[6].

У Швеції законодавчий орган з метою транспонування Директиви 2006/24[7] до національного законодавства вніс поправки до Закону (2003) про електронні комунікації та Регламенту (2003) про електронні комунікації. Обидва ці документи містять правила зберігання даних електронних комунікацій і доступу до них національних органів. Йдеться про дані, що стосуються під-

[6] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) <https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng> (accessed 27.03.2026).

[7] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (No longer in force) <https://eur-lex.europa.eu/eli/dir/2006/24/oj/eng> (accessed 27.03.2026).

писок і всіх електронних повідомлень, необхідних для відстеження та ідентифікації джерела і призначення повідомлення; визначення його дати, часу і типу; ідентифікації використовуваного обладнання зв'язку та визначення місцезнаходження обладнання мобільного зв'язку, що використовується на початку і наприкінці кожного повідомлення. Дані, що підлягають зберіганню, – це дані, створені або оброблені в контексті послуг телефонного зв'язку, послуг телефонного зв'язку з використанням мобільного зв'язку, систем електронних повідомлень, послуг доступу до Інтернету та послуг надання пропускної здатності інтернет-доступу (режим з'єднання).

Щодо послуг телефонного зв'язку, що використовують мобільний зв'язок, накладаються додаткові зобов'язання, що охоплюють, наприклад, збереження даних про місцезнаходження на початку і наприкінці сеансу зв'язку. Щодо послуг телефонного зв'язку, що використовують IP-пакет, дані, що підлягають зберіганню, включають, крім згаданих вище даних, дані про IP-адреси абонентів, що викликають і викликаються. Стосовно систем електронних повідомлень дані, що підлягають зберіганню, включають дані про номери відправників і одержувачів, IP-адреси або інші адреси для відправлення повідомлень. Стосовно послуг доступу до Інтернету, дані, що підлягають зберіганню, включають, наприклад, дані про IP-адреси користувачів, а також відстежувані дати і час входу в систему та виходу з неї.

Водночас у Регламенті Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний регламент про захист даних)[8] визначено, що обробка персональних даних повинна бути спрямована на служіння людству. *Право на захист персональних даних не є абсолютним;* воно повинно розглядатися у зв'язку з його функцією в суспільстві та *бути збалансованим з іншими основними правами відповідно до принципу пропорційності.* Державам дозволяється зберігати та вводити нові положення для подальшого уточнення застосування правил Регламенту. Також не виключається законодавство держав-членів, яке встановлює обставини для конкретних ситуацій обробки, зокрема, більш точне визначення умов, за яких обробка персональних даних є законною. Підвищений рівень захисту встановлений для особливої категорії даних, зокрема, забороняється обробка персональних даних, що розкривають расове або етнічне походження, політичні переконання, релігійні або філософські переконання, членство в профспілках, а також обробка генетичних даних, біометричних даних з метою унікальної ідентифікації фізичної особи, даних про здоров'я або про статеве життя або сексуальну орієнтацію особи. Водночас ця вимога не застосовується, якщо обробка є необхідною з міркувань істотного су-

[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) <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> (accessed 27.03.2026).

спільного інтересу на підставі законодавства Союзу або держави-члена, яке має бути пропорційним для поставленої мети (п. g ч. 2 ст. 9).

Заслуговує на увагу позиція, відповідно до якої рішення про застосування такої міри, як обмеження конфіденційності, приймається керівником відповідного органу або особою, якій делеговані ці повноваження. Рішення не підлягає попередньому розгляду судовим органом або незалежним адміністративним органом.

У контексті збору розвідувальної інформації національна поліція, Säkerhetspolisen (Служба безпеки Швеції) та Tullverket (Митна служба Швеції) можуть на підставі п. 1 Закону (2012), на умовах, передбачених цим законом, і без повідомлення постачальника електронної комунікаційної мережі або постачальника послуг електронної комунікації здійснювати збір даних, що стосуються повідомлень, переданих електронною комунікаційною мережею, електронного комунікаційного обладнання, розташованого в зазначеному географічному районі, та географічних районів, де знаходиться або знаходилося електронне комунікаційне обладнання. Відповідно до пунктів 2 і 3 Закону (2012) *дані, як правило, можуть бути зібрані, якщо, залежно від обставин, ця міра є особливо необхідною для запобігання, запобігання або розкриття злочинної діяльності, пов'язаної з одним або декількома злочинами, що караються позбавленням волі на строк не менше двох років, або одним із діянь, перелічених у п. 3 цього закону, що належать до злочинів, які караються позбавленням волі на строк менше двох років. Будь-які підстави для застосування цього заходу повинні переважати міркування, що стосуються шкоди або збитків, які можуть бути заподіяні особі, на яку поширюється даний захід, або інтересам, що протистоять цьому заходу.* Відповідно до п. 5 цього закону тривалість застосування даного заходу не повинна перевищувати одного місяця. Рішення про застосування такої міри приймається керівником відповідного органу або особою, якій делеговані ці повноваження. Рішення не підлягає попередньому розгляду судовим органом або незалежним адміністративним органом.

За законодавством Великої Британії, такий доступ до інформації є можливим від будь-якої поштової служби та телекомунікаційної служби, якщо цього потребують: інтереси національної безпеки; запобігання або розкриття злочину або запобігання безладам; інтереси економічного добробуту Сполученого Королівства; інтереси громадської безпеки; захист громадського здоров'я; оцінка або збір будь-якого податку, мита, збору або іншого оподаткування, внеску або платежу, що підлягає сплаті державному департаменту; мета, в надзвичайній ситуації, запобігти смерті або травмі або будь-якій шкоді фізичному або психічному здоров'ю людини, або пом'якшити будь-яку травму або шкоду фізичному або психічному здоров'ю людини.

Суд ЄС визначає, що ст. 15(1) Директиви 2002/58 дозволяє державам-членам обмежувати сферу дії принципового зобов'язання щодо забезпечення

pravoua.com.ua

конфіденційності повідомлень і пов'язаних з ними даних про трафік, це положення має, відповідно до усталеної прецедентної практики Суду, тлумачитися суворо[9]. З огляду на серйозність втручання в основні права, передбачені національним законодавством, яке з метою боротьби зі злочинністю передбачає збереження даних про трафік і місцезнаходження, тільки мета боротьби з тяжкими злочинами може виправдати такий захід[10].

Право Європейського Союзу передбачає в надзвичайних ситуаціях доступ до персональних даних усіх осіб, які користуються послугами електронного зв'язку, навіть, якщо ці особи не перебувають, навіть опосередковано, у ситуації, яка може спричинити кримінальне переслідування. Право на доступ до персональних даних уповноваженим органом є всеосяжним, оскільки стосується персональних даних усіх осіб, які користуються послугами електронного зв'язку, навіть, якщо ці особи *не перебувають, навіть опосередковано, у ситуації, яка може спричинити кримінальне переслідування.* Отже, воно застосовується навіть до осіб, стосовно яких відсутні докази, які дають підстави припустити, що їхня поведінка може мати зв'язок, нехай навіть непрямий або віддалений, з тяжкими кримінальними злочинами. Крім того, воно не передбачає жодних винятків і, отже, застосовується навіть до осіб, чиї повідомлення, згідно з нормами національного права, підпадають під зобов'язання збереження професійної таємниці.

Крім того, хоча ефективність боротьби з тяжкими злочинами, зокрема з організованою злочинністю та тероризмом, може значною мірою залежати від використання сучасних методів розслідування, така мета загального інтересу, якою б фундаментальною вона не була, сама по собі не може виправдати те, що національне законодавство, яке передбачає загальне й невибіркове зберігання всіх даних про трафік і місцезнаходження, має вважатися необхідним для цілей цієї боротьби.

Стаття 15(1) Директиви 2002/58, розглянута у світлі статей 7, 8 і 11, а також ст. 52(1) Хартії основоположних прав ЄС[11], не перешкоджає державі-члену приймати законодавство, що дозволяє як превентивний захід цілеспрямоване зберігання даних про трафік і місцезнаходження з метою боротьби з тяжкими злочинами, за умови, що зберігання даних обмежується суворою необхідністю щодо категорій даних, які підлягають зберіганню, задіяних засобів зв'язку, зацікавлених осіб і встановленого періоду зберігання.

Додаткові правила встановлюються для регулювання обробки персональних даних у різних сферах. Так, Директивою (ЄС) 2016/681 Європей-

[9] Josef Probst v mr.nexnet GmbH, Case C-119/12, Judgment of 22 November 2012, ECLI:EU:C:2012:748 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0119> (accessed 27.03.2026).

[10] Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others, Joined Cases C-293/12 and C-594/12, Judgment of 8 April 2014, ECLI:EU:C:2014:238 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293> (accessed 27.03.2026).

[11] Charter of Fundamental Rights of the European Union <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> (accessed 27.03.2026).

ського Парламенту та Ради від 27 квітня 2016 р. про використання даних реєстрації пасажирів (PNR) для запобігання, виявлення, розслідування та переслідування терористичних актів і тяжких злочинів[12] значно розширені можливості для опрацювання інформації, що надаються авіакомпаніями органам безпеки держав. Обмін даними про пасажирів є корисним для запобігання, виявлення та судового переслідування терористичних актів і тяжких злочинів. Директива про систему реєстрації пасажирів спрямована на регулювання передачі цих базових даних авіакомпаніями національним органам влади, тоді як Правила попередньої інформації про пасажирів (API) встановлюють правила збору та передачі більш широкого спектра персональних даних національним органам влади.

Дані запису реєстрації пасажира – це персональні дані, що надаються пасажирами, які збираються та зберігаються авіакомпаніями. Ці дані включають у себе різні відомості, такі як ім'я пасажира, дати поїздки, маршрут, номер місця, відомості про багаж, контактну інформацію та використовуваний спосіб оплати. Директива регулює передачу цих даних правоохоронним органам держав-членів та їх обробку з метою запобігання та виявлення злочинів терористичного характеру або тяжких форм злочинів, а також для проведення розслідувань і судового переслідування в цій сфері.

Ефективне використання даних, наприклад, шляхом порівняння з різними базами даних про розшукуваних осіб та об'єкти, необхідне для запобігання, виявлення, розслідування та судового переслідування терористичних актів і тяжких злочинів і, отже, для зміцнення внутрішньої безпеки, збору доказів і, за необхідності, пошуку спільників злочинців і розкриття злочинних мереж. Для запобігання, виявлення, розслідування та судового переслідування терористичних актів і тяжких злочинів усім державам-членам необхідно ввести положення, що зобов'язують авіаперевізників, які виконують рейси за межі ЄС, передавати зібрані ними дані. Державам-членам також слід надати можливість поширити це зобов'язання на авіаперевізників, які виконують рейси всередині ЄС.

Термін зберігання даних повинен бути таким, щоб він був співмірний цілям запобігання, виявлення, розслідування та судового переслідування терористичних актів і тяжких злочинів. З огляду на характер даних та їх використання необхідно, щоб дані зберігалися достатньо довго для проведення аналізу та використання в розслідуваннях. Щоб уникнути непропорційного використання, після закінчення початкового терміну зберігання дані слід деперсоналізувати шляхом маскування окремих елементів даних. Для забезпечення найвищого рівня захисту даних доступ до повних даних PNR, що дають змогу безпосередньо ідентифікувати суб'єкта даних, повинен на-

[12] Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime <https://eur-lex.europa.eu/eli/dir/2016/681/oj> (accessed 27.03.2026).

pravoua.com.ua

даватися тільки при дотриманні дуже суворих і обмежених умов після закінчення початкового терміну.

Директива не впливає на можливість держав-членів передбачати в рамках свого національного законодавства систему збору та обробки даних від економічних операторів, які не є перевізниками, таких як туристичні агентства та туроператори, що надають послуги, пов'язані з поїздками, включаючи бронювання рейсів, для яких вони збирають та обробляють дані, або від постачальників транспортних послуг, інших, ніж ті, що зазначені в цій Директиві, за умови, що таке національне законодавство відповідає праву Союзу.

Авіаперевізники повинні передавати дані PNR електронним способом з використанням загальних протоколів і підтримуваних форматів даних, які будуть прийняті відповідно до процедури перевірки, зазначеної в ст. 17(2), або, у разі технічного збою, будь-якими іншими відповідними способами, що забезпечують належний рівень безпеки даних: 1) *за 24–48 годин до запланованого часу вильоту рейсу;* 2) *відразу після закриття рейсу, тобто як тільки пасажири сіли в літак, готуючись до вильоту, і посадка або висадка пасажирів більше неможлива.* У випадках, коли доступ до даних необхідний для реагування на конкретну і реальну загрозу, пов'язану з терористичними актами або тяжкими злочинами, авіаперевізники повинні в кожному конкретному випадку передавати дані PNR у моменти часу, відмінні від зазначених у правилах ЄС, на запит відповідно до національного законодавства.

Такий механізм оцінки даних дає змогу ідентифікувати осіб, які до проведення такої оцінки не підозрювалися в причетності до терористичних злочинів або тяжких злочинів і які повинні бути піддані подальшій перевірці компетентними органами. Це дає змогу протидіяти загрозі терористичних злочинів і тяжких злочинів з іншої точки зору, ніж при обробці інших категорій персональних даних. Однак для забезпечення того, щоб обробка даних PNR обмежувалася необхідним, створення та застосування критеріїв оцінки повинні бути обмежені терористичними злочинами та тяжкими злочинами, для яких використання таких критеріїв є актуальним.

Попередня інформація про пасажира стосується особи пасажира, яку зазвичай отримують з проїзних документів або паспортів, наприклад, повне ім'я, дата народження, національність. Ця інформація передається державним органам і може стати корисним інструментом для урядів при здійсненні прикордонного контролю або забезпеченні безпеки. У грудні 2022 р. Комісія прийняла законопроєкти з регулювання, спрямовані на спрощення управління зовнішніми кордонами та зміцнення внутрішньої безпеки. У 2024 р.

Рада та Європейський Парламент досягли згоди щодо нової законодавчої бази[13].

Більшість держав-членів уже використовують дані про пасажирів, що передаються в поліцію або інші органи влади відповідно до національного законодавства. Система PNR ЄС гармонізує правові положення держав-членів, уникаючи правової невизначеності та прогалин у безпеці, забезпечуючи при цьому захист даних. ЄС уже підписав угоди, що дають змогу європейським перевізникам передавати дані до США та Австралії. У квітні 2025 р. Рада прийняла рішення, яке офіційно укладає угоду між ЄС і Канадою про передачу та використання даних пасажирів.

Директива про реєстрацію пасажирських перевезень спрямована на регулювання передачі даних авіакомпаніями національним органам влади, а також обробки цих даних цими органами. Згідно з цією Директивою авіакомпанії зобов'язані надавати дані про пасажирів на рейсах до ЄС і з ЄС. Держави-члени мають право, але не зобов'язані, збирати дані для деяких рейсів всередині ЄС.

Директива встановлює, що зібрані дані можуть оброблятися тільки з метою запобігання та виявлення терористичних злочинів і тяжких форм злочинів, а також для проведення розслідувань і судового переслідування в цій сфері. У рамках цієї діяльності дані можуть бути використані декількома способами: 1) з метою оцінки ризику, який становлять пасажири до їх прибуття або до їх відправлення з урахуванням певних критеріїв ризику або з метою ідентифікації конкретних осіб; 2) для розробки цих критеріїв ризику; 3) у контексті конкретних розслідувань або судових переслідувань.

Дані про пасажирів, що збираються авіаперевізниками, та до яких мають доступ уповноважені органи: локатор записів, дата бронювання / видачі квитка, дата передбачуваної поїздки, ім'я, адреса та контактна інформація (номер телефону, адреса електронної пошти), усі форми платіжної інформації, включаючи платіжну адресу, повний маршрут подорожі для конкретного, інформація про пасажирів, які часто літають, туристичне агентство / турагент, статус поїздки пасажира, включаючи підтвердження, статус реєстрації, інформацію про неявку або явку, загальні зауваження (включаючи всю доступну інформацію про неповнолітніх без супроводу дорослих віком до 18 років, таку як ім'я та стать неповнолітнього, вік, мова, якою він розмовляє, ім'я та контактні дані опікуна при виїзді та його ставлення до неповнолітнього, ім'я та контактні дані опікуна при прибутті та його ставлення до неповнолітнього, агент з виїзду та прибуття), номер місця та інша інформація про місце, вся інформація про багаж, а також попередньо зібрану інформацію про подорожі (тип, номер, країну видачі та дату закінчення тер-

[13] Pact on Migration and Asylum. A common EU system to manage migration. 21 May 2024 <https://home-affairs.ec.europa.eu/policies/migration-and-asylum/pact-migration-and-asylum_en#timeline-and-main-achievements> (accessed 27.03.2026).

pravoua.com.ua

міну дії будь-якого документа, що посвідчує особу, громадянство, прізвище, ім'я, стать, дату народження, авіакомпанію, номер рейсу, дату відправлення, дату прибуття, порт відправлення, порт прибуття, час відправлення та час прибуття).

В Європейському Союзі встановлено перелік правопорушень, які дають підстави для збору персональних даних: участь у злочинній організації; торгівля людьми; сексуальна експлуатація дітей і дитяча порнографія; незаконний обіг наркотичних засобів і психотропних речовин; незаконний обіг зброї, боєприпасів і вибухових речовин; корупція; шахрайство, зокрема проти фінансових інтересів Союзу; відмивання доходів, отриманих злочинним шляхом, та підробка валюти, включаючи євро; комп'ютерні злочини / кіберзлочинність; екологічні злочини, включаючи незаконну торгівлю видами тварин, що перебувають під загрозою зникнення, а також видами і сортами рослин, що перебувають під загрозою зникнення; сприяння несанкціонованому в'їзду і проживанню; вбивство, тяжкі тілесні ушкодження; незаконна торгівля людськими органами і тканинами; викрадення людей; незаконне позбавлення волі і захоплення заручників; організоване й озброєне пограбування; незаконний обіг культурних цінностей, включаючи антикваріат і твори мистецтва; контрафактна та піратська продукція; підробка адміністративних документів та торгівля ними; незаконний обіг гормональних речовин та інших стимуляторів росту; незаконний обіг ядерних або радіоактивних матеріалів; зґвалтування; *злочини, що підпадають під юрисдикцію Міжнародного кримінального суду;* незаконне захоплення літаків / суден; саботаж; торгівля викраденими транспортними засобами; промислове шпигунство.

В умовах протистояння загрозам держави зобов'язані класифікувати як терористичні злочини всі правопорушення, якщо вони вчиняються з конкретною терористичною метою, а саме: серйозно залякати населення, неправомірно примусити державні органи або міжнародну організацію до вчинення або утримання від вчинення будь-якої дії, або серйозно дестабілізувати чи зруйнувати основні політичні, конституційні, економічні або соціальні структури країни чи міжнародної організації. Загроза вчинення таких умисних дій також повинна розглядатися як терористичний злочин, якщо на підставі об'єктивних обставин установлено, що така загроза була висловлена однією з цих терористичних цілей[14].

Аналогічний досвід щодо розширення повноважень правоохоронних органів у питаннях одержання доступу до персональних даних з метою боротьби зі злочинністю чи в інших надзвичайних ситуаціях є у США. Після серії терактів та появи нових викликів і загроз для США 26 жовтня 2001 р.

[14] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA <https://eur-lex.europa.eu/eli/dir/2017/541/oj> (accessed 27.03.2026).

Конгресом було ухвалено Закон "Об'єднання та зміцнення Америки шляхом надання відповідних інструментів, необхідних для перешкоджання та запобігання тероризму" (USA PATRIOT Act) з метою запобігання та покарання терористичних актів у Сполучених Штатах та в усьому світі, вдосконалення інструментів правоохоронних органів для проведення розслідувань та з інших цілей[15]. Цим законом було суттєво розширено повноваження відповідних уповноважених органів щодо збору персональних даних, що зумовлено фактичними або потенційними атаками чи іншими серйозними ворожими діями іноземної держави або агенту іноземної держави; саботажу або міжнародного тероризму з боку іноземної держави або агенту іноземної держави; або таємної розвідувальної діяльності розвідувальної служби або мережі іноземної держави або агенту іноземної держави з урахуванням вірогідності створювати ризики для національної оборони або безпеки, здійснення дій, як можуть впливати на зовнішню політику тощо. На підставі цього Закону надавач послуг може надавати персональні дані урядовій установі, якщо є підстави вважати, що надзвичайна ситуація, яка становить безпосередню загрозу смерті або серйозного фізичного ушкодження будь-якій особі, виправдовує розкриття інформації. Постачальник електронних комунікаційних послуг або послуг віддаленого обчислення повинен розкривати записи або іншу інформацію, що стосується абонента або клієнта таких послуг.

Висновки. З метою розширення повноважень правоохоронних органів України (на що вказує Європейська Комісія у звітах від 30 жовтня 2024 р.[16] та 4 листопада 2025 р.[17]) в умовах воєнного стану об'єктивно виправданим і необхідним є ухвалення Закону України "Про тимчасове обмеження захисту персональних даних в умовах воєнного стану" за досвідом США та держав – членів Європейського Союзу, в якому передбачити можливість обмеження гарантій конфіденційності персональних даних у надзвичайних ситуаціях та під час воєнного стану; рішення про застосування такої міри (обмеження конфіденційності) приймається керівником відповідного органу або особою, якій делеговані ці повноваження (таким органом, наприклад, може стати СБУ); рішення не підлягає попередньому розгляду судовим органом або незалежним адміністративним органом; за стандартами ЄС передбачити право у надзвичайних ситуаціях мати уповноваженим органам доступ до персональних даних усіх осіб, які користуються послугами електронного зв'язку, навіть якщо ці особи не перебувають, навіть опосередковано, у ситуації, яка може спричинити кримінальне переслідування.

[15] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001 <https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf> (accessed 27.03.2026).

[16] European Commission, 2024 Communication on EU enlargement policy. Brussels, 30.10.2024 COM(2024)690 <https://enlargement.ec.europa.eu/2024-communication-eu-enlargement-policy_en> (accessed 27.03.2026).

[17] European Commission, Ukraine Report 2025. Brussels, 4.11.2025 SWD(2025)759 <https://enlargement.ec.europa.eu/ukraine-report-2025_en> (accessed 27.03.2026).

Nataliia Akhtyrska
Bogdan Ostudimov

LIMITATIONS ON DATA PRIVACY GUARANTEES IN EMERGENCY SITUATIONS AND DURING MARTIAL LAW: EU LAW AND US EXPERIENCE

Abstract. International standards for safeguarding and ensuring human rights are based on the presumption of a shared understanding of the value of the rule of law and the potential application, in the event of a conflict of interests, of a regulated procedure for resolving imbalances. A particular challenge arises during armed conflict, when matters of national security take precedence.

As historical experience shows, during war, the enemy side employs methods to undermine statehood, intimidate the population, and create the impression that law enforcement agencies are incapable of taking measures to prevent and combat crime, conducting effective investigations, or ensuring that courts deliver just verdicts. To this end, they resort to terrorist threats and other actions, with the aim of seriously destabilising or destroying the country's fundamental political, constitutional, economic or social structures.

According to the Office of the Attorney General, 608,101 criminal offences were recorded in 2025, of which 154,093 were particularly serious crimes and 304,667 were serious crimes. Under martial law, crimes against the foundations of Ukraine's national security (5,404), crimes against public safety (8,989) and others pose a particular threat. In Ukraine in 2025, 1,070 cases of treason (Article 111 of the Criminal Code of Ukraine) and 1,714 cases of collaboration were detected, and 160 criminal offences were recorded under Article 258 of the Criminal Code of Ukraine ("Terrorist Act"), etc. At the same time, the number of criminal proceedings in which cases have been referred to court is significantly lower (of 608,101 proceedings, 139,707 were referred to court with an indictment), which indicates certain procedural obstacles in the collection of evidence. The legislature has introduced amendments to procedural legislation that take into account the specific features of pre-trial investigations under martial law; however, the duration of hostilities has created additional risks and challenges, including in the rear, through the detonation of explosives during the transport of postal items, the use of Ukrainians' SIM cards for intelligence purposes, and so on. Martial law and other states of emergency, based on the experience of other states, provide grounds for the legislator to introduce mechanisms for ensuring state security that are proportionate to the threats.

Keywords: personal data; restrictions on confidentiality; martial law; extended access to data for a range of persons without a ruling by an investigating judge.

ПРАВО УКРАЇНИ • 2026 • № 3 • 155-167