

ЗАХИСТ ЖУРНАЛІСТСЬКИХ ДЖЕРЕЛ: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ

Аналітичне дослідження

2026



Лабораторія
цифрової
безпеки

ZMІNA
ЦЕНТР ПРАВ ЛЮДИНИ



Фінансується
Європейським Союзом

Авторка — Анна Людва, юристка

Рецензентки

Тетяна Авдєєва, старша юристка,
Віта Володовська, голова організації

Лабораторія цифрової безпеки

Анотація

Документ аналізує європейські стандарти захисту журналістських джерел і конфіденційних комунікацій, закріплені в Європейському акті про свободу медіа (EMFA), практиці Європейського суду з прав людини, актах Ради Європи та законодавстві держав-членів Європейського Союзу. У дослідженні розглянуто поняття журналістських джерел, коло суб'єктів, на яких поширюються гарантії захисту, заборонені форми втручання в журналістську діяльність, умови правомірного розкриття джерел, а також стандарти щодо застосування заходів стеження та судового контролю.

Окрему увагу приділено аналізу українського законодавства в контексті зобов'язань України як держави-кандидата на вступ до ЄС. Дослідження виявляє ключові прогалини національного регулювання та оцінює його відповідність вимогам EMFA і європейським стандартам свободи медіа. На основі проведеного аналізу сформульовано рекомендації щодо вдосконалення законодавства України, спрямовані на забезпечення ефективного захисту журналістських джерел, конфіденційних комунікацій та гарантій незалежної журналістської діяльності.

Документ підготовлено у співпраці з Центром прав людини ZMINA за фінансової підтримки Європейського Союзу. Його зміст є виключною відповідальністю Лабораторії цифрової безпеки і не обов'язково відображає позицію Європейського Союзу.

Захист журналістських джерел — одна з фундаментальних гарантій свободи вираження поглядів, свободи медіа та права суспільства на отримання інформації. Можливість журналістів збирати, перевіряти та поширювати інформацію значною мірою залежить від довіри джерел до конфіденційності їх взаємодії з медіа. Саме тому захист журналістських джерел посідає центральне місце в практиці Європейського суду з прав людини (ЄСПЛ, Суд), стандартах Ради Європи та праві Європейського Союзу (ЄС).

Важливим етапом розвитку європейських стандартів у цій сфері стало ухвалення Європейського акта про свободу медіа (European Media Freedom Act, EMFA), який уперше на рівні ЄС встановив комплексні мінімальні гарантії захисту журналістських джерел і конфіденційних комунікацій. EMFA не лише закріплює заборону на втручання в журналістську діяльність через вимогу розкрити джерела, проведення обшуків, вилучення матеріалів чи застосування засобів стеження, але й визначає вичерпні умови, за яких такі втручання можуть бути допустимими.

Для України питання захисту журналістських джерел набуває особливо значення в контексті європейської інтеграції та виконання зобов'язань держави як країни-кандидата на вступ до ЄС. Попри наявність окремих гарантій у національному законодавстві, чинна правова рамка не забезпечує комплексного та системного захисту журналістських джерел і конфіденційних комунікацій відповідно до стандартів EMFA та практики ЄСПЛ.

Мета цього дослідження — проаналізувати європейські стандарти захисту журналістських джерел і конфіденційних комунікацій, закріплені в EMFA, практиці ЄСПЛ, актах Ради Європи та законодавстві держав-членів ЄС, а також оцінити відповідність українського законодавства цим стандартам і підготувати рекомендації для його вдосконалення.

ЖУРНАЛІСТСЬКІ ДЖЕРЕЛА ЯК ОБ'ЄКТ ЗАХИСТУ

[EMFA](#) став першим актом на рівні ЄС, що впроваджує мінімальні стандарти захисту журналістських джерел і конфіденційних комунікацій. Відповідно до його преамбули, джерела інформації є своєрідною «сировиною» для журналістів: вони формують основу для створення медіаконтенту, зокрема новинного контенту та матеріалів з актуальних суспільно важливих питань. Тому вкрай важливо забезпечити захист можливості журналістів збирати, перевіряти достовірність й аналізувати інформацію, зокрема надану або передану конфіденційно, як в онлайн-, так і офлайн-середовищі, яка стосується журналістських джерел або може дозволити їх ідентифікувати. EMFA не надає визначення конфіденційних комунікацій, проте захищає відповідну інформацію еквівалентно із журналістськими джерелами. З інших європейських документів впливає, що до таких комунікацій [входить](#) будь-яка інформація конфіденційної природи, якою обмінюються або яка передається сторонами за допомогою загальнодоступних електронних комунікаційних послуг.

На рівні Ради Європи [Рекомендація № R\(2000\)7 «Про право журналістів не розкривати свої джерела інформації»](#) (Рекомендація) заохочує держави-члени забезпечити чіткий і прозорий захист права журналістів на нерозкриття «інформації, що ідентифікує джерело». Такий підхід також врахований у практиці ЄСПЛ, який здебільшого посилається на Рекомендацію при аналізі справ щодо правомірності розкриття журналістських джерел у межах статті 10 Конвенції про захист прав людини і основоположних свобод (Конвенція). Суд зазначає, що конфіденційність журналістських джерел стосується не лише прав журналістів, а й більшою мірою самих джерел, які добровільно допомагають їм в інформуванні громадськості про предмет публічного інтересу¹. У цьому випадку Рекомендація тлумачить термін «джерело» як «*будь-яку особу, яка передає інформацію журналістові*». Аналогічного підходу [дотримується](#) і ЄСПЛ. До «інформації, що ідентифікує джерело» в Рекомендації віднесено:

- (1) ім'я та персональні дані, а також голос та зображення джерела;
- (2) фактичні обставини одержання журналістом інформації від джерела²;

¹ *Stichting Ostade Blade v the Netherlands (dec.)*, 8406/06, para. 64, *Nordisk Film & TV A/S v Denmark (dec.)*, 40485/02, *Guide on Article 10 of the European Convention on Human Rights / Freedom of expression*, para. 356.

² *Görmüş and Others v Turkey*, 49085/07, para. 45, *Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands*, 39315/06, para. 86, *Guide on Article 10 of the European Convention on Human Rights / Freedom of expression*, para. 358.

- (3) неопублікований зміст інформації, що передається журналістові від джерела,³ та
- (4) персональні дані журналістів та їхніх роботодавців, пов'язані зі здійсненням журналістами їхньої професійної діяльності.

Важливо, що не кожному особу, яку журналіст використовує для отримання інформації, можна вважати «джерелом» у розумінні практики ЄСПЛ.

Статус «джерело» надається лише у випадку **добровільного та свідомого надання інформації**.

Наприклад, у скарзі [Nordisk Film & TV A/S v Denmark](#), де журналіст перебував під прикриттям, особи, які надавали інформацію, не знали, що вони говорять із журналістом, таким чином, не давали згоди на відео чи запис і відповідно надання інформації. Суд визнав скаргу неналежно обґрунтованою з огляду на те, що особи, які надали інформацію, не вважалися джерелами журналістської інформації в традиційному розумінні.

Інший важливий фактор — **мотивація джерела інформувати громадськість про предмет публічного інтересу**.

У скарзі [Stichting Ostade Blade v the Netherlands](#), яка була визнана неприйнятною, Суд не розглядав контекст «захисту джерел», оскільки інформатор, який визнав у листі до медіапредставників власну відповідальність за серію бомбових атак, не був мотивований бажанням надати інформацію, а навпаки — шукав публічного розголосу нападів під прикриттям преси.

На рівні національного регулювання підходи держав-членів ЄС залишаються фрагментованими. Поряд із законодавчими рамками, які є досить загальними, важливе значення має судова практика.

У [Німеччині](#) «джерелом» інформації є автор, розповсюдjuвач коментарів і документації або будь-який інший інформатор (ст. 53(1) 2). Під інформацією розуміється контент, матеріали та документація, які пройшли редакційну перевірку. До останніх [входить](#) контент, що міститься

³ *Ibis*.

в письмовій формі, на аудіо- чи візуальних носіях, на носіях даних, у зображеннях чи іншому матеріалізованому контенті або передається незалежно від способу зберігання за допомогою інформаційних чи комунікаційних технологій (ст. 11(3)). Таким чином, захист журналістських джерел [поширюється](#) і на фотожурналістику: постачальники зображень, як-от фотоагентства або фотографи, вважаються джерелами в традиційному сенсі. Утім, якщо через публікацію фотографій відбулося втручання в інтимну сферу життя третіх осіб без наявності публічного інтересу, такі дії можуть виходити за межі захисту журналістських джерел, передбачені законодавством (детальніше про правомірні випадки розкриття джерел у Розділі 4)⁴.

Визначення «джерела» в [Нідерландах](#) віддзеркалює критерії ЄСПЛ щодо вільного й цілеспрямованого волевиявлення особи в наданні інформації суспільного інтересу. В Ірландії положення щодо захисту журналістських джерел законодавчо закріплено лише на рівні Конституції і то непрямо. Так званий журналістський привілей, тобто можливість збереження конфіденційності джерел, поширюється як на особу джерела, так і на інформацію, передану ним журналістам або видавцям⁵.

Натомість у [Бельгії](#) діє чи не єдиний у Європі спеціальний закон, що регулює захист журналістських джерел, уповноважує журналістів не розкривати власні джерела або інформацію, записи та документи, які можуть:

- ◆ розкрити особу їхніх інформаторів;
- ◆ розкрити характер або походження їхньої інформації;
- ◆ розкрити особу автора тексту чи аудіовізуальної продукції;
- ◆ розкрити зміст самої інформації та документів, якщо вони ідентифікують інформатора (ст. 3).

Інші держави-члени ЄС використовують загальні поняття та детально не роз'яснюють, яка інформація підлягає захисту. Наприклад, закон Італії [надає](#) обмежений захист «джерелу» та стосується ідентифікації лише «імені та прізвища» (пара. 31). Згідно з [австрійським законом](#), суб'єкти захисту в контексті надання показань під час судових проваджень мають право відмовитися відповідати на запитання про особу автора, відправника або джерела статей та документації чи будь-якої інформації,

⁴ *Regional Court Munich I, Judgment of 11 September 2003 — 7 O 20974/02.*

⁵ *Constitution of Ireland, Art. 40, Cornec v Morrice and Others ([2012] IEHC 376).*

отриманої для здійснення їхньої професійної діяльності (ст. 31). З подальших статей можна зробити висновок, що до такої інформації належать документи, друковані матеріали, носії зображень, звуку або даних, ілюстрації та інший контент. У [Данії](#) схожа практика: журналісти не зобов'язані свідчити щодо особи джерела інформації, автора статті або особи, яка зробила фотографію чи створила інший образотворчий матеріал (ст. 172). До джерела інформації закон відносить і особу, зображення якої показано або яка є (була) предметом відповідної розмови. Згідно із [законом Швеції](#), не можна розголошувати інформацію про особу, яка створила продукцію або зробила її доступною для публікації, брала участь у такій публікації або повідомила інформацію медіа (ст. 3).

[Фінляндія](#) загалом захищає конфіденційність джерела інформації в повідомленні, зокрема вимагаючи не розкривати особу ініціатора повідомлення (ст. 16). [Закон Мальти](#) також обмежується захистом джерела вже опублікованої інформації, яка «міститься в газеті, трансляції чи на вебсайті», без захисту джерел на стадії її підготовки (ст. 22). Натомість [Хорватія](#) захищає як уже опубліковану інформацію, так і матеріал, який планується опублікувати (ст. 30).

ЖУРНАЛІСТИ, МЕДІА ТА ІНШІ ОСОБИ ЯК СУБ'ЄКТИ ЗАХИСТУ

EMFA поширює гарантії захисту на провайдерів медіасервісів, їхній редакційний персонал, а також на інших осіб, які через свої регулярні приватні або професійні відносини з провайдерами медіапослуг або членами їхніх редакцій можуть володіти інформацією, за допомогою якої можна ідентифікувати журналістські джерела або конфіденційні комунікації.

Провайдери медіасервісів

«Провайдер медіасервісів» — це фізична або юридична особа, професійною діяльністю якої є надання медіапослуги та яка несе редакційну відповідальність за вибір змісту медіапослуги і визначає спосіб її організації. В Україні відповідно до Закону «Про медіа» до таких провайдерів можна віднести суб'єкти у сфері аудіовізуальних, друкованих та онлайн-медіа, попри відсутність формально закріпленого терміна.

На рівні ЄС тільки [Угорщина](#) поширює захист від розкриття журналістських джерел лише на «провайдерів медіаконтенту», які фактично означають провайдерів медіасервісів (ст. 6). Таке обмежувальне

застосування закону пов'язане як із недосконалою законодавчою рамкою, так і домінантними політичними настроями.

Редакційний персонал провайдерів медіасервісів

До редакційного персоналу ЕМФА відносить журналістів (зокрема, і тих, хто працює за нестандартними формами зайнятості, як-от фрилансерів) і редакторів. Визначення «журналіст» в ЕМФА не передбачено, а на європейському рівні дефініція варіює. Найбільш поширеним [залишається](#) визначення журналіста як «*будь-якої фізичної або юридичної особи, яка регулярно або професійно займається збором та поширенням інформації серед громадськості через будь-які засоби масової комунікації*».

[Закон Німеччини](#) фактично повторює це визначення: особа, яка професійно займається «підготовкою, виробництвом або розповсюдженням друкованої продукції, передач або наданням інформаційно-комунікаційних послуг, пов'язаних з навчанням чи формуванням громадської думки» (ст. 53(1)(5), проте не вживає терміна «журналіст» задля уникнення його обмежувального застосування. Аналогічно [Швеція](#) поширює захист на осіб, які брали участь у виробництві або розповсюдженні продукції (у тому числі друкованої), що містить або призначена для формування частини програми чи технічного запису (ст. 3).

Оскільки право журналістів не розкривати свої джерела інформації є професійним привілеєм, мета якого — заохочення джерел надавати важливу інформацію в конфіденційний спосіб, «нежурналісти» (наприклад, фізичні особи, які ведуть власний вебсайт чи блог) [не мають змоги](#) реалізувати відповідне право. На противагу такій практиці яскравим прикладом слугують [Нідерланди](#), чий кримінальний закон поширює захист журналістських джерел і конфіденційних комунікацій на «журналістів і публіцистів», не надаючи визначення цим термінам задля уникнення обмежувального тлумачення (ст. 218а). У такому випадку [використовується](#) широке тлумачення терміна «журналіст» — особа, яка залучена в професійну звітність подій, що покриває не лише працівників медіа, а і фотографів, операторів, карикатуристів, письменників, творців програм, блогерів та влогерів. Утім, така практика скоріше виняток із правил. Наприклад, [Італія](#) аналогічно захищає «журналістів і публіцистів» на законодавчому рівні, проте застосування закону залишається обмеженим відповідними суб'єктами.

[Французький Закон про свободу преси](#) визначає «журналіста» як особу, яка на регулярній і платній основі збирає інформацію та поширює її серед громадськості, здійснюючи свою професійну діяльність в онлайн-, аудіовізуальних або пресагенціях (ст. 2). Аналогічного

підходу дотримується й [Бельгія](#), відносячи до журналістів самозайнятих або найманих осіб, включно з юридичними особами, які регулярно та безпосередньо збирають, пишуть або поширюють інформацію через медіа на благо громадськості (ст. 2). [Закон Хорватії](#) сформульований у схожій формі, проте захисту підлягають лише фізичні особи (ст. 2). [Австрійський Закон про медіа](#) поширює свій захист на власників медіа, редакторів та працівників медіапідприємства чи медіаслужби (ст. 31(1)). За [фінським законом](#), автор повідомлення для громадськості, видавець і мовник мають право зберігати конфіденційність джерела інформації (ст. 16).

[Мальтійський закон](#) поширює свою дію лише на редактора, автора, видавця або оператора вебсайту, без зазначення інших медіаакторів (ст. 22). [Данія](#) надає захист тільки редакторам і редакційним працівникам, що працюють у друкованому виданні та радіо- або телевізійному підприємстві. В Ірландії через відсутність законодавчої рамки вимоги Конституції поширюють свою дію лише на журналістів і «нежурналістів видавців, які виконують демократичну та освітню функцію, передбачену Конституцією»⁶.

Інші особи, які через свої регулярні приватні або професійні відносини з провайдером медіасервісів або його редакційним персоналом можуть мати інформацію для розкриття.

Рекомендація [обмежена](#) захистом осіб, які можуть мати відомості про джерела через «*свої професійні зв'язки із журналістами*», натомість EMFA розширює сферу захисту, включаючи як осіб, що проживають у спільному будинку на стабільній та постійній основі, так і осіб, які на професійній основі займаються підготовкою, виробництвом або розповсюдженням програм або пресрелізів. До персоналу провайдерів медіасервісів може належати також технічний колектив, зокрема експерти з питань кібербезпеки.

Говорячи про національну практику держав-членів ЄС, зазначимо, що [французький закон](#) захищає осіб, які можуть мати відомості про журналістські джерела через «постійні відносини із журналістом» (ст. 2). [Нідерландський закон](#) захищає осіб, які збирають, зберігають або редагують відповідну інформацію перед публікацією: документалістів, редакторів офісу та співробітників секретаріату. Такої ж практики дотримується і [Бельгія](#), проте використовує інше формулювання: захисту підлягає персонал редакції, який «*виконуючи свої обов'язки, змушений ознайомлюватися з інформацією, що може призвести до ідентифікації джерела*» шляхом збору,

⁶ Constitution of Ireland, Art. 40, *Cornec v Morrice and Others* ([2012] IEHC 376).

обробки та поширення такої інформації (ст. 2). У [Хорватії](#) право на нерозкриття поширюється на головного редактора, редакторів та авторів опублікованих матеріалів, які не є журналістами (ст. 30). У [Фінляндії](#) таким правом наділені особи, які працюють на автора повідомлення, видавця або мовника (ст. 16). У [Швеції](#) — особи, які будь-яким чином беруть активну участь у роботі підприємства, що виробляє технічні записи або транслює програми, або в інформаційному агентстві (ст. 3).

[Мальтійський закон](#) також може поширювати свій захист на осіб, які через свої приватні або професійні відносини з провайдером медіасервісів чи його редакційним персоналом (працівниками або підрядниками) володіють інформацією, за допомогою якої можна встановити особу журналістського джерела (ст. 22). [Данія](#) поширює захист на осіб, які «через свій зв'язок» із виданням або теле-, радіокомпанією дізналися про особу джерела або автора, утім, не уточнює суть відповідних «зв'язків» (ст. 172(3)).

ЗАБОРОНЕНІ ЗАХОДИ ЩОДО МЕДІА ТА ЖУРНАЛІСТІВ

ЕМФА містить вичерпний перелік заходів, які вживаються до медіа та журналістів обмежено. По-перше, заборонено **вимагати від провайдерів медіасервісів або їхнього редакційного персоналу розкриття журналістських джерел або конфіденційних комунікацій чи звертатися з аналогічною вимогою до осіб, які можуть мати доступ до такої інформації через свої приватні або професійні відносини.**

У своїй практиці ЄСПЛ дотримується досить однозначного підходу, загалом забороняючи національним органам вимагати розкриття журналістських джерел. Суд [стверджує](#), що захист журналістських джерел є однією з основних умов свободи преси, без існування якої джерела можуть відмовитися допомагати в інформуванні громадськості щодо питань публічного інтересу.

«Беручи до уваги важливість захисту журналістських джерел для свободи преси в демократичному суспільстві та потенційно охолоджувальний вплив наказу про розкриття джерел на реалізацію цієї свободи, такий захід не може бути сумісним зі статтею 10 Конвенції, якщо він не виправданий переважачою вимогою публічного інтересу» (Goodwin v the United Kingdom, 17488/90, пара. 39).

Примітно, що право журналістів не розкривати свої джерела [поширюється](#) також на джерела з поліції чи судових органів: у випадку потенційно незаконного отримання інформації журналістом на противагу розкриттю джерел вимагається провести внутрішнє розслідування органами правопорядку.

На рівні практики держав-членів ЄС існують загальні вимоги щодо нерозкриття журналістських джерел здебільшого в контексті кримінальних або адміністративних проваджень. Наприклад, відповідно до [Акта про медіа та дифамацію Мальти](#), жоден суд чи трибунал, передбачений законом, не може вимагати від редактора, автора, видавця чи оператора вебсайту розкривати джерела інформації, що міститься в газеті, трансляції чи вебсайті, за які він відповідальний, за відсутності легітимних підстав (ст. 22). У таких країнах, як Австрія, Данія, Нідерланди, Фінляндія та Угорщина (проте лише у виняткових випадках), під час судових проваджень суб'єкти захисту звільняються від обов'язку надавати показання щодо джерела інформації або інформації, яка може допомогти ідентифікувати відповідну особу.

По-друге, до заборонених заходів EMFA відносить **затримання, накладення санкцій, перехоплення або перевірку** провайдерів медіасервісів або їхнього редакційного персоналу, **здійснення спостереження, обшуку або вилучення їхніх корпоративних або приватних приміщень із метою отримання інформації, пов'язаної із журналістськими джерелами чи конфіденційними комунікаціями**, або вжиття аналогічних заходів щодо осіб, які можуть мати доступ до такої інформації через приватні або професійні відносини.

Зростання впливу технологічних можливостей не може виправдовувати перехоплення листування, стеження за журналістами або обшук та вилучення їхньої конфіденційної інформації. ЄСПЛ указав, що обшуки житлових і робочих місць журналістів із метою ідентифікації осіб, які надали їм конфіденційну інформацію, є втручанням у право на свободу вираження поглядів⁷.

Здійснення обшуків із метою ідентифікації джерела інформації [загрожує](#) захисту джерел більшою мірою, ніж наказ, який вимагає розкрити особу інформаторів.

Такого висновку Суд дійшов у справі [Görmüş and Others v Turkey](#), де органи прокуратури з метою встановлення посадових осіб, які надали

⁷ *Roemen and Schmit v Luxembourg*, 51772/99, пара. 47, *Ernst and Others v Belgium*, 33400/96, пара. 94, *Tillack v Belgium*, 20477/05, пара. 56.

конфіденційну інформацію, несподівано з'явилися на робочих місцях журналістів, провели обшук та вилучення документів, копіювання на зовнішні диски всього вмісту їхніх комп'ютерів та надалі зберігали такі диски (пара. 57). Відповідно до рішення суду, «...слідчі, які з ордером на проведення обшуку несподівано з'являються на робоче місце журналіста, мають надзвичайно широкі повноваження здійснення розслідування, оскільки, таким чином, вони мають доступ до всієї наявної у журналіста документації»⁸. У цьому випадку ЄСПЛ [звертає](#) увагу на нецільовий збір будь-якої інформації, яку має журналіст, під час обшуків — фактор, який перетинає межу правомірного розкриття журналістських джерел.

Примітно, що вжиті заходи [будуть](#) інтрузивними навіть за умови безуспішних обшуків, які, утім, мають на меті ідентифікацію джерела. У справі [Voskuil v the Netherlands](#), де журналіста було ув'язнено більш ніж на два тижні, щоб примусити його розкрити джерело інформації, ЄСПЛ дійшов висновку, що такі далекосяжні заходи лише перешкоджають особам, які мають правдиву та точну інформацію, виступати й ділитися нею з пресою в майбутніх справах (пара. 71).

Говорячи про національну практику держав-членів ЄС, зазначимо, що [Кримінальний процесуальний кодекс Німеччини](#) встановлює чітку заборону на вилучення документів, носіїв звуку, зображень та інших матеріалів, що перебувають у журналістів та медіапрацівників або в редакції, видавництвах, друкарні чи телерадіокомпанії (ст. 97(5)). Вилучення, здійснене всупереч цій забороні, призводить до неприйнятності доказів у кримінальному провадженні. Понад те, обшуки в редакціях із метою пошуку доказів неприпустимі, якщо ці заходи спеціально спрямовані на матеріали та інформацію, що охороняються кримінальним законом⁹.

[Кримінальний процесуальний кодекс Нідерландів](#) забороняє вилучати матеріали та обшукувати робочі місця журналістів і публіцистів. Така заборона реалізується, навіть якщо самі дії не спрямовані на ідентифікацію джерел, проте існує велика ймовірність несанкціонованого доступу до захищеної інформації. Аналогічні заборони передбачені законом Бельгії. Данія та Угорщина наразі забороняють лише вилучення речей із метою розкриття джерел осіб, які перебувають під захистом через свою журналістську діяльність.

Нарешті, EMFA забороняє **розгортати інтрузивне програмне забезпечення для здійснення стеження** за будь-якими матеріалами, цифровими пристроями, машинами або інструментами, що використовуються

⁸ *Roemen and Schmit v Luxembourg*, 51772/99, пара. 57.

⁹ *Federal Constitutional Court of Germany, Judgment of 27 February 2007 — 1 BvR 538/06, 1 BvR 2045/06.*

провайдерами медіасервісів, їхнім редакційним персоналом або особами, які можуть мати доступ до такої інформації через приватні або професійні відносини. Особливості цих обмежень розглянемо детальніше далі.

ЛЕГІТИМНІ ПІДСТАВИ ДЛЯ РОЗКРИТТЯ ЖУРНАЛІСТСЬКИХ ДЖЕРЕЛ

EMFA передбачає вичерпний перелік умов, за яких держави-члени ЄС можуть відступити від вимог щодо захисту журналістських джерел. Такий відступ повинен:

1. Бути передбаченим положеннями закону ЄС або національного закону.

На рівні держав-членів ЄС положення, які дозволяють відступати від заходів, заборонених EMFA, містяться здебільшого в кримінальному процесуальному законодавстві, рідше в медійних законах. У більшості країн відступ виправдовується вимогами пропорційності та суттєвого суспільного інтересу при розслідуванні серйозних злочинів. Деякі країни, як-от Мальта та Хорватія, надають широке поле для маневрів, дозволяючи розкривати журналістські джерела задля національної безпеки, територіальної цілісності тощо. Радше винятком із правил є Швеція, яка забороняє будь-яке обмеження конфіденційності джерел на конституційному рівні, та Австрія, яка передбачає абсолютне право на захист журналістських джерел без концепту балансування інтересів.

Для оцінки легітимності втручання в права журналістів ЄСПЛ використовує трискладовий тест, який враховує, окрім передбаченості втручання законом, також критерій переслідування легітимної мети та необхідність втручання в демократичному суспільстві. Практика демонструє, що в контексті легітимної мети національні органи здебільшого [посилаються](#) на «захист національної безпеки» та «запобігання розголошенню інформації, отриманої конфіденційно». У цьому випадку ЄСПЛ наголошує на необхідності «*стриманого застосування терміна [національна безпека] та його обмеженого тлумачення, застосовуючи його, як це було продемонстровано, тільки тоді, коли це необхідно для запобігання опублікуванню такої інформації з метою захисту національної безпеки*»¹⁰.

¹⁰ *Görmüş and Others v Turkey*, 49085/07, пара. 37.

2. Відповідати вимогам статті 52(1) Хартії основних прав ЄС щодо дотримання принципів пропорційності та необхідності при обмеженні прав.

Положення [Хартії основних прав ЄС](#) (Хартія), на яке посилається ЕМФА, встановлює, що будь-яке обмеження в здійсненні прав і свобод, гарантованих цією Хартією, має бути передбачене законом та не порушувати сутність цих прав і свобод. За умови дотримання принципу пропорційності такі обмеження можуть встановлюватися лише тоді, коли вони необхідні та справді відповідають цілям загального інтересу, визнаним ЄС, або потребі захисту прав і свобод інших осіб.

У більшості держав-членів ЄС розкриття джерел може бути виправданим заходом у випадку розслідування серйозних кримінальних правопорушень, відповідальність за які передбачає позбавлення волі на строк, який варіює залежно від законодавства держави-члена. У Нідерландах таке покарання становить 12 років, у Німеччині — 5 років (для випадків, коли йдеться про вилучення матеріалів), у Данії та Фінляндії — 4 роки або більше та 6 років відповідно (але лише у випадку, коли вимагається розкриття джерел під час надання свідчень).

У [Німеччині](#) вимога розкрити джерела вважатиметься виправданою, якщо вона пов'язана із запобіганням або розслідуванням серйозного кримінального правопорушення, наприклад злочину проти миру та загрози демократичній державі, державної зради та загрози зовнішній безпеці, злочину проти статевого самовизначення та відмивання коштів (ст. 53). Додатково заходи, спрямовані на розкриття джерел, [вважатимуться виправданими](#), якщо розслідування фактів та обставин або розслідування місцезнаходження обвинуваченого інакше буде безуспішним або більш ускладненим.

У [Бельгії](#) до таких злочинів відносять терористичні злочини, перелік яких міститься в законі (наприклад, взяття в заручники, масове знищення, захоплення повітряного судна, випущення небезпечних субстанцій у повітря тощо) (ст. 137). У [Швеції](#) в такому списку злочини виняткової важливості, як-от повстання, державна зрада, іноземне шпигунство, несанкціоноване поводження із секретною інформацією (ст. 4).

Радше недосконалими положеннями вирізняється [Угорщина](#), чий спеціальний закон дозволяє розкривати відповідні джерела в судовому порядку у випадках, дозволених законом, з метою розслідування злочину (ст. 6(2)). Утім, закон не уточнює, про розслідування яких злочинів йдеться, що розширює дискрецію органів правопорядку.

Оцінюючи критерій необхідності втручання, ЄСПЛ враховує обставини конкретної справи. У скарзі *Nordisk Film & TV A/S v. Denmark*, визнаній неприйнятною, Суд [дійшов висновку](#), що втручання в права журналіста шляхом розкриття його джерел було виправданим, оскільки мета таких дій полягала в запобіганні кримінальним правопорушенням, у тому числі серйозному випадку сексуального насильства над неповнолітніми. ЄСПЛ [додав](#), що вимога розкрити джерела стосувалася лише дослідницьких матеріалів заявника, пов'язаних із діяльністю підозрюваної кримінальної організації, а невідредаговані записи та нотатки, зроблені журналістом-заявником, могли допомогти розслідуванню та наданню доказів.

3. Бути виправданим переважаючим суспільним інтересом та пропорційним.

На рівні Ради Європи значна увага приділяється критеріям пропорційності та переважаючого суспільного інтересу, оскільки вони оцінюються та аналізуються з огляду на індивідуальні обставини конкретної справи. Рекомендація [вказує](#), що право журналістів не розголошувати конфіденційну інформацію підлягає винятково обмеженням статті 10(2) Конвенції: відповідна інформація може бути розкрита, якщо для цього існує переважаючий суспільний інтерес, а обставини мають достатньо важливий та серйозний характер. Відповідно до [Рекомендації](#), розкриття інформації, що ідентифікує джерело, вважається необхідним, якщо (1) зважених заходів, альтернативних розкриттю, не існує або вони вже вичерпані особами чи органами державної влади, які намагалися її розкрити, і (2) законний інтерес у розкритті очевидно переважає суспільний інтерес у нерозкритті, враховуючи, що:

- ◆ необхідність розкриття переважає потребу захисту джерел;
- ◆ обставини мають надзвичайно важливий та серйозний характер;
- ◆ необхідність розкриття визначена як така, що відповідає нагальній суспільній потребі, та
- ◆ держави-члени користуються певною свободою розсуду в оцінці такої потреби, але ця свобода нерозривно пов'язана з наглядом із боку ЄСПЛ.

У випадку видання наказу про розкриття журналістських джерел національні органи [повинні надати](#) обґрунтовані причини переважаючого суттєво важливого інтересу над інтересом нерозголошення та вичерпання альтернативних заходів (наприклад, використання інших доказів).

Національні закони держав-членів ЄС аналогічно враховують критерій переважаючого суспільного інтересу. Наприклад, у Німеччині постачальники фотографій вважаються «джерелами», проте захист обмежений втручанням публікацією таких фотографій у приватну сферу життя третьої особи без наявного публічного інтересу¹¹.

[Закон Хорватії](#) дозволяє розкривати джерела на вимогу суду, якщо такий захід необхідний для захисту суспільного інтересу та стосується особливо важливих і серйозних обставин, з урахуванням того, що (1) альтернативних заходів розкриттю не існує або їх вичерпано та (2) суспільний інтерес у розкритті джерела переважає інтерес у захисті конфіденційної інформації (ст. 30(5)).

Натомість французьке законодавство містить загальні терміни, що призводить до широкого тлумачення та, як наслідок, свавільного втручання в роботу журналістів органами правопорядку. Відповідно до [французького закону](#), таємниця джерел може бути порушена прямо чи опосередковано лише у випадку, якщо це виправдовує переважаючий імператив публічного інтересу та якщо передбачувані заходи суворо необхідні та пропорційні переслідуюній законній меті (ст. 2). При цьому таке втручання жодним чином не може полягати у зобов'язанні журналіста розкривати свої джерела. Утім, практика демонструє часте зловживання нечіткою концепцією «переважаючого імперативу публічного інтересу» через відсутність належного захисту конфіденційних матеріалів журналістів. Наприклад, у 2023 році органи безпеки [обшукали](#) помешкання або перевірили комп'ютери кількох журналістів, щоб отримати доступ до інформації про їхні джерела. Одним із найвідоміших випадків було [розслідування](#) журналістки видання *Disclosure* Аріан Лаврільє про порушення державної таємниці під час висвітлення продажу Францією зброї за кордон та участі військових в операції, що призвела до вбивства мирних жителів у Єгипті. Через відмову розкрити власні джерела за журналісткою стежили протягом кількох років, обшукували її будинок, вивчали соціальні мережі та телефон, а надалі заарештували та тримали під вартою 39 годин.

4. Підлягати попередній авторизації судовим органом або незалежним і неупередженим органом або у виняткових і термінових випадках — подальшій авторизації такими органами без затримки.

Забезпечення належного рівня захисту журналістських джерел і конфіденційних комунікацій вимагає, щоб заходи для отримання такої

¹¹ *Regional Court Munich I, Judgment of 11 September 2003 — 7 O 20974/02.*

інформації були санкціоновані органом, який може незалежно й неупереджено оцінити, чи вони виправдані переважаючим суспільним інтересом, наприклад судом, суддею, прокурором, який діє як суддя, або іншим подібним органом, уповноваженим санкціонувати такі заходи відповідно до національного законодавства. Детальніше ці гарантії захисту розглянемо в розділі про судовий захист.

СТЕЖЕННЯ ЗА МЕДІА ТА ЖУРНАЛІСТАМИ З МЕТОЮ РОЗКРИТТЯ ЇХНІХ ДЖЕРЕЛ

EMFA встановлює чітку заборону на **розгортання інтрузивного програмного забезпечення для здійснення стеження** за будь-якими матеріалами, цифровими пристроями, машинами або інструментами, що використовуються провайдерами медіасервісів, їхнім редакційним персоналом або особами, які можуть мати доступ до такої інформації через приватні або професійні відносини. В обмежених випадках стеження може застосовуватися, якщо розгортання інтрузивного програмного забезпечення:

- ◆ відповідає умовам, переліченим у попередньому розділі, а також
- ◆ здійснюється з метою розслідування щодо одного із захищених суб'єктів (провайдера медіасервісів, представника його редакційного персоналу або особи, яка може мати доступ до конфіденційних комунікацій через свої приватні або професійні відносини), якщо йдеться про:
- ◆ злочини з переліку [Рамкового рішення ЄС](#), які караються позбавленням волі або триманням під вартою строком щонайменше на 3 роки, або
- ◆ інші тяжкі злочини, які караються позбавленням волі або триманням під вартою строком щонайменше на 5 років.

Таким чином, для розгортання програмного забезпечення для інтрузивного стеження необхідно встановити, чи досягає правопорушення, про яке йде мова, порогу серйозності, встановленого в EMFA, чи може воно, після індивідуальної оцінки всіх відповідних обставин у конкретній справі, бути підставою для розслідування та чи кримінальне переслідування цього правопорушення заслуговує на особливо нав'язливе втручання в основоположні права та економічні свободи, яке передбачає використання програмного забезпечення

для інтрузивного стеження, чи є достатні докази того, що відповідне правопорушення було скоєно, і чи є використання програмного забезпечення для інтрузивного стеження важливим для встановлення фактів, пов'язаних із розслідуванням та кримінальним переслідуванням цього правопорушення.

Розглядаючи справи щодо використання заходів стеження, ЄСПЛ також приділяє чималу увагу правовій основі й чіткості законодавчих положень, які уповноважують на відповідні заходи. За загальним правилом, закон повинен передбачати щонайменше: (1) характер правопорушень; (2) визначення категорій осіб, які можуть стати суб'єктами стеження; (3) тривалість відповідних заходів; (4) процедуру використання та зберігання отриманих даних; (5) запобіжні заходи при передачі даних іншим сторонам та (6) обставини, за яких отримані дані повинні бути видалені або знищені¹².

У [Дослідженні щодо використання системи Pegasus та аналогічного шпигунського стеження](#) Європейський парламент наголошує на гарантіях для суб'єктів стеження. Відповідно до дослідження, заходи стеження повинні залишатися винятковим заходом, якому передують судова авторизація незалежного органу з належною оцінкою необхідності та пропорційності. Такі заходи [повинні бути](#) «суворо обмежені справами, що стосуються національної безпеки або пов'язані з тероризмом та серйозними злочинами». Водночас парламент закликає держави-члени необґрунтовано не посилатися на «національну безпеку» для виправдання заходів стеження. Відповідна концепція [повинна трактуватися](#) більш обмежено: просте посилання на «національну безпеку» не може тлумачитися як необмежений виняток із застосування права ЄС, а повинно вимагати чіткого обґрунтування. Таким чином, концепт «національної безпеки» [не має збігатися](#) з концептом «внутрішньої безпеки», який охоплює набагато ширшу рамку (наприклад, більше видів злочинів) щодо загроз відповідній країні.

Практика ЄСПЛ у контексті розгляду справ щодо стеження за медіа та журналістами також демонструє потребу в ефективних процесуальних гарантіях для суб'єктів стеження, причому реалізованих до розгортання відповідних інтрузивних заходів. ЄСПЛ [наголошує](#), що таргетоване спостереження повинне підлягати попередньому нагляду незалежного органу, який уповноважений на авторизацію або припинення стеження. У такому випадку нагляд, здійснений пост-фактум, вважатиметься неефективним. Наприклад, у справі [Bucur and Toma v Romania](#), де військовий підрозділ розвідувальної служби

¹² Kennedy v the United Kingdom, 26839/05, para. 231.

прослуховував телефони великої кількості журналістів, політиків і бізнесменів, ЄСПЛ визнав порушення, оскільки не було отримано жодних необхідних дозволів та не існувало жодних індикаторів або доказів загрози національній безпеці, яка могла б виправдати перехоплення телефонних розмов (пара. 120). ЄСПЛ [наголошує](#), що таємне стеження допускається лише за умови суворої необхідності. Таким чином, оцінка правомірності заходів залежить від усіх обставин справи: характеру, обсягу та тривалості заходів, правової основи, механізму нагляду та способів правового захисту¹³.

Вищезгадана справа відрізняється від скарги [Weber and Saravia v Germany](#), де Суд аналізував німецьке законодавство, яке уповноважує органи безпеки на здійснення стратегічного моніторингу шляхом перехоплення телекомунікацій. Згідно з німецьким законом, такий моніторинг правомірний лише у випадку збору інформації для запобігання тяжким злочинам, зокрема збройному конфлікту, міжнародному тероризму, нелегальному імпорту наркотичних засобів, відмиванню коштів тощо (пара. 26–27). На відміну від попередньої справи, тут ЄСПЛ визнав, що заходи органів безпеки були спрямовані лише на збір інформації про запобігання вищезгаданим злочинам, а не розкриття журналістських джерел. Утім, навіть за цієї умови Суд [підтвердив](#), що німецький закон містив гарантії щодо збереження таємниці телекомунікацій медіа, як-от використання отриманих даних лише для запобігання певним серйозним кримінальним злочинам, для зведення розкриття журналістських джерел до неминучого мінімуму (пара. 152).

Говорячи про практику держав-членів ЄС, звернемо увагу, що більшість країн імплементувала законодавчі положення щодо заходів стеження, на які уповноважені здебільшого органи правопорядку та служби безпеки, проте зловживання повноваженнями та вдавання до шпигунських технологій і надалі регулярно трапляються. Це зумовлено здебільшого зростанням тенденцій до інкорпорації технологій у роботу безпекових органів: наприклад, у січні 2026 року уряд Ірландії [оголосив](#) про роботу над законопроектом, який уповноважує поліцію на здійснення шпигунського стеження.

Згідно з [грецьким законом](#), конфіденційність комунікацій може бути порушена з міркувань національної безпеки та для розслідування певних злочинів (ст. 254(1)(d), 255 (1)(b)). Закон не уточнює тяжкість або ступінь злочинів, для розслідування яких органи можуть вдаватися до інтрузивних заходів, що призводить до стеження у випадку

¹³ *Klass and Others v Germany*, 5029/71, пара. 50.

незначних правопорушень або проступків. Понад те, запит осіб щодо інформації про те, чи зазнавали вони стеження з міркувань національної безпеки, [розглядає](#) комітет із трьох членів — директора служби безпеки, прокурора та керівника регулятора у сфері комунікацій. Оскільки до складу комітету щодо розгляду запитів входить особа, яка вимагає здійснення стеження (директор служби безпеки), та особа, яка авторизує відповідні заходи (прокурор), [виникають](#) очевидні сумніви в неупередженості та об'єктивності відповідного органу. У справах, що стосуються національної безпеки, відповідній особі [повідомляють](#) про здійснення за нею стеження через три роки після завершення заходів, за умови, що це не ставить під загрозу мету, для якої було призначено заходи.

Проблематичні аспекти спостерігаються і в законодавстві Угорщини. Угорський Закон про поліцію [вимагає](#) попередньої судової авторизації при здійсненні заходів стеження, проте якщо заходи мають запобігти тероризму, відповідну авторизацію натомість надає міністр юстиції. ЄСПЛ [визнав](#), що політичний характер дозволу міністра збільшує ризик зловживань і не забезпечує необхідних гарантій незалежності, неупередженості та належної процедури. Ба більше, угорський закон [не містить](#) вимог щодо повідомлення суб'єктів спостереження із чіткою вказівкою, що цільових осіб не треба інформувати про те, що за ними ведеться стеження.

Аналогічно польський Закон про поліцію, який слугує правовою основою для здійснення органами правопорядку оперативного спостереження, [не містить](#) достатніх гарантій для запобігання неправомірному втручанням в приватність осіб. Аналіз польського закону [продемонстрував](#), що попередня судова авторизація, потрібна перед вжиттям заходів стеження, слугує здебільшого формальним фактором і залежить більшою мірою від політичних настроїв.

ПРАВО НА СУДОВИЙ ЗАХИСТ ПРОТИ НЕПРАВОМІРНИХ ЗАХОДІВ

ЕМФА наголошує, що провайдери медіасервісів, їхній редакційний персонал або особи, які можуть мати доступ до конфіденційної інформації через свої приватні або професійні відносини, мають **право на ефективний судовий захист**. Відповідне положення охоплює як засоби захисту *ex ante* (до порушення), так і засоби захисту *ex post* (після порушення) відповідно до [статті 47 Хартії](#).

Одна з процедурних гарантій *ex ante* — **попередня судова авторизація заходів**, або **перегляд заходів**, пов'язаних із розкриттям журналістських джерел і конфіденційних комунікацій **незалежним і неупередженим органом**. Такий орган повинен бути інституційно відокремленим від виконавчої влади та інших зацікавлених сторін і наділеним повноваженнями визначати наявність суспільного інтересу в джерелах, які вимагають розкрити, до здійснення такого розкриття. ЄСПЛ підкреслив обов'язковість попереднього перегляду заходів навіть у термінових випадках, який буде ефективним для запобігання невиправданому витоку інформації із джерел. «На думку Суду, очевидно, що здійснення будь-якого незалежного перегляду, який відбувається лише після передачі матеріалів, здатних розкрити такі джерела, підриває саму сутність права на конфіденційність»¹⁴.

ЕМФА також наголошує на тому, що заходи стеження підлягають регулярному перегляду незалежним органом, щоб з'ясувати, чи зберігаються умови, що виправдовують застосування відповідного заходу. Ця вимога також виконується, якщо мета регулярного перегляду полягає в перевірці того, чи були виконані умови, що виправдовують продовження терміну дії дозволу на застосування заходу.

З метою ефективного здійснення права на судовий захист важливо своєчасно інформувати, без шкоди для ефективності поточних розслідувань, про заходи, вжиті без відома зацікавленої особи. Такий спосіб захисту має особливе значення для тих, хто став або потенційно може стати суб'єктом стеження, у тому числі журналістів.

Оскарження заходів особами, щодо яких були здійснені заходи, спрямовані на втручання в їхню журналістську діяльність, — інша процесуальна гарантія згідно з ЕМФА. Утім, практика держав-членів ЄС демонструє, що відповідні гарантії надаються здебільшого всім суб'єктам, щодо яких здійснюються заборонені заходи, особливо в контексті правоохоронної діяльності. Наприклад, закон Німеччини, який регулює обмеження таємниці кореспонденції та телекомунікацій органами безпеки, уповноважує незалежну комісію розглядати скарги щодо прийнятності або правомірності обмежувальних заходів (ст. 15). Понад те, у випадку вдавання до заходів стеження парламентська Рада нагляду що шість місяців отримує від федерального міністра, уповноваженого на авторизацію заходів стеження, звітність про такі заходи (ст. 14).

¹⁴ *Sanoma Uitgevers B.V. v the Netherlands [GC], 38224/03, пара. 91.*

УКРАЇНСЬКИЙ КОНТЕКСТ І РЕКОМЕНДАЦІЇ

Як країна-кандидат до ЄС, Україна перебуває на активній стадії гармонізації національного законодавства з європейськими стандартами. Останні містять і положення про захист журналістських джерел і конфіденційних комунікацій, передбачені EMFA.

Наразі українське законодавство здебільшого не враховує основних вимог EMFA, хоча формально право журналіста «не розкривати джерело інформації або інформацію, яка дозволяє встановити джерела інформації, крім випадків, коли його зобов'язано до цього рішенням суду на основі закону» закріплене в [Законі України «Про інформацію»](#) (ст. 25(3)) та [Законі України «Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста»](#) (ст. 11-1). Окрім того, [Кримінальний процесуальний кодекс](#) (КПК) відносить журналістські джерела до охоронюваної законом таємниці (ст. 162). Утім, перелік суб'єктів, на яких поширюється захист, обмежений лише журналістами. Оскільки EMFA таким захистом охоплює й провайдерів медіасервісів, право не розкривати конфіденційну інформацію в Україні повинно поширюватися і на окремих «суб'єктів у сфері медіа» з урахуванням їхньої професійної діяльності та редакційних зобов'язань, передбачених [Законі України «Про медіа»](#).

До того ж українське законодавство не містить переліку заборонених заходів щодо медіапрацівників і легітимних винятків, коли розкриття журналістських джерел і конфіденційних комунікацій буде вважатися виправданим. Відповідні заходи наразі передбачені [Законі України «Про оперативно-розшукову діяльність»](#) лише для негласних слідчих розшукових дій, як-от аудіо- та відеоконтроль особи, зняття інформації з електронних комунікаційних мереж, накладення арешту на кореспонденцію особи тощо (ст. 8).

Також в українському законодавстві немає визначення інтрузивного стеження, у тому числі з використанням програмного забезпечення, як і процесуальних гарантій у випадку вдавання до таких заходів. Суттєвою проблемою залишається відсутність належного нагляду з боку незалежного органу для забезпечення правомірності заходів, на чому наголосив і ЄСПЛ у рішенні [Sedletska v Ukraine](#) (щодо несанкціонованого доступу до даних телефона журналістки). Також відсутні положення про попередній перегляд заходів, коли оцінюється, чи були збалансовані публічні інтереси та інтереси нерозкриття журналістських джерел. Наразі через ці законодавчі прогалини органи правопорядку можуть здійснювати нецільовий збір інформації, яку мають журналісти,

посилаючись на формальні приводи щодо захисту внутрішньої або національної безпеки.

Враховуючи європейські стандарти та найкращу практику держав-членів ЄС, **Лабораторія цифрової безпеки рекомендує українським законотворцям:**

1. Розширити коло суб'єктів, на яких поширюються гарантії захисту журналістських джерел і конфіденційних комунікацій.
2. Визначити чіткий перелік заборонених заходів на законодавчому рівні.
3. Внести зміни до КПК та інших законів щодо умов застосування заходів, спрямованих на розкриття інформації про журналістські джерела й конфіденційні комунікації.
4. Внести зміни до КПК та інших законів щодо посилення гарантій судового контролю у випадку застосування заходів, спрямованих на розкриття інформації про журналістські джерела й конфіденційні комунікації.
5. Використовувати на законодавчому рівні обмежене визначення концепту національної безпеки в контексті заходів, спрямованих на розкриття інформації про журналістські джерела й конфіденційні комунікації.
6. Визначити в КПК перелік правопорушень, розслідування яких легітимізує заходи, спрямовані на розкриття інформації про журналістські джерела й конфіденційні комунікації.
7. Передбачити законодавчу вимогу щодо надання обґрунтованих і достатніх причин від органів правопорядку у випадку запиту на розкриття журналістських джерел, а також пояснення, чому таку інформацію неможливо отримати шляхом альтернативних або менш інтрузивних заходів.
8. Законодавчо визначити поняття програмного забезпечення для інтрузивного стеження та умови його застосування.
9. Встановити гарантії права журналіста та інших суб'єктів, що захищаються, на інформацію про будь-яку обробку персональних даних, що здійснюється в контексті застосування заходів стеження, у тому числі за допомогою програмного забезпечення.

10. Переглянути та внести зміни до інших законів для узгодження використання нових термінів і понять. Зокрема, внести до КПК узгоджені зміни, що стосуються захисту журналістської діяльності.
11. Розробити та впровадити навчальні програми для суддів про застосування норм законодавства щодо захисту журналістських джерел і конфіденційних комунікацій.
12. Розробити та впровадити навчальні програми для органів прокуратури про застосування норм законодавства щодо захисту журналістських джерел і конфіденційних комунікацій.
13. Передбачити регулярний моніторинг та аналіз стану дотримання вимог захисту журналістських джерел і конфіденційних комунікацій.



Лабораторія
цифрової
безпеки

ZMІNA
ЦЕНТР ПРАВ ЛЮДИНИ



Фінансується
Європейським Союзом