ГАРАНТІЇ ЗАХИСТУ КОНФІДЕНЦІЙНОСТІ КОМУНІКАЦІЙ ЖУРНАЛІСТІВ У КРИМІНАЛЬНОМУ ПРОЦЕСІ: ЄВРОПЕЙСЬКІ СТАНДАРТИ ТА РЕКОМЕНДАЦІЇ ДЛЯ УКРАЇНИ

Аналітичне дослідження

2026

Лабораторія цифрової безпеки

ZMINA
ЦЕНТР ПРАВ ЛЮДИНИ

Фінансується Європейським Союзом

Автори:

Максим Дворовий, юрист Лабораторії цифрової безпеки
Владислав Левчук
Анна Максимчук

Рецензенти:

Тетяна Авдєєва, юристка Лабораторії цифрової безпеки
Віта Володовська, голова Лабораторії цифрової безпеки

Анотація

Документ присвячений аналізу європейських стандартів захисту конфіденційності журналістських комунікацій та журналістських джерел у контексті застосування заходів таємного стеження. На основі практики Європейського суду з прав людини (ЄСПЛ) та положень Європейського акта про свободу медіа (EMFA) досліджуються мінімальні гарантії й запобіжники, необхідні для законного використання негласних заходів спостереження, зокрема щодо журналістів та медіаорганізацій. Особливу увагу приділено критеріям санкціонування стеження, механізмам незалежного контролю, захисту конфіденційних комунікацій, повідомленню осіб про втручання та доступним засобам правового захисту. Дослідження також оцінює відповідність чинного кримінального процесуального законодавства України європейським стандартам і пропонує комплекс рекомендацій щодо внесення змін до Кримінального процесуального кодексу України для посилення гарантій захисту журналістських джерел, обмеження використання інтрузивного програмного забезпечення для стеження та забезпечення балансу між потребами кримінального правосуддя, національної безпеки та свободою медіа.

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

ВСТУП

Конфіденційність комунікацій журналістів і захист журналістських джерел — одні з ключових передумов функціонування незалежних медіа та реалізації права суспільства на отримання інформації. У демократичному суспільстві журналісти виконують роль суспільних посередників, забезпечуючи громадський контроль над діяльністю державних органів, політичних діячів та інших впливових суб'єктів. Можливість виконувати цю функцію значною мірою залежить від здатності журналістів гарантувати своїм джерелам конфіденційність та захист від розкриття.

Розвиток цифрових технологій суттєво змінив характер ризиків для журналістської діяльності. Якщо раніше втручання в конфіденційність комунікацій здебільшого обмежувалося прослуховуванням телефонних розмов або вилученням документів, то сьогодні органи правопорядку та служби безпеки можуть використовувати значно більш інтрузивні інструменти, у тому числі програмне забезпечення для прихованого доступу до цифрових пристроїв, перехоплення зашифрованих повідомлень, отримання геолокаційних даних та дистанційну активацію мікрофонів і камер. Такі заходи створюють безпрецедентні ризики для конфіденційності журналістських джерел, а отже — і для свободи медіа загалом.

Європейський суд з прав людини (ЄСПЛ, Суд) сформував розгалужену практику щодо допустимості заходів таємного стеження та гарантій захисту права на повагу до приватного життя і свободи вираження поглядів. Суд послідовно наголошує, що системи прихованого стеження можуть бути сумісними з вимогами Конвенції про захист прав людини і основоположних свобод (Конвенція) лише за наявності чіткої правової основи, ефективного незалежного контролю, процесуальних гарантій від зловживань та ефективних засобів правового захисту. Водночас Європейський акт про свободу медіа (EMFA) встановив додаткові спеціальні гарантії для журналістів та медіа, зокрема щодо використання програмного забезпечення для інтрузивного стеження та втручання в конфіденційні комунікації.

Для України питання захисту конфіденційності журналістських комунікацій набуває особливого значення з кількох причин. По-перше, Україна перебуває на етапі адаптації національного законодавства до права Європейського Союзу в межах процесу вступу до ЄС. По-друге, повномасштабна війна та посилення ролі правоохоронних і безпекових органів об'єктивно збільшують ризики втручання в приватні комунікації та використання інструментів стеження. По-третє, практика ЄСПЛ у справах проти України вже вказала на наявність низки системних проблем у сфері правового регулювання та контролю за здійсненням негласних слідчих (розшукових) дій.

Мета цього дослідження — аналіз європейських стандартів застосування заходів таємного стеження та захисту конфіденційності журналістських комунікацій, визначення ключових вимог ЄСПЛ та EMFA, а також того, наскільки вони враховані в чинному кримінальному процесуальному законодавстві України. Особливу увагу приділено гарантіям проти зловживань під час здійснення таємного стеження, умовам використання інтрузивного програмного забезпечення щодо журналістів та необхідним змінам до Кримінального процесуального кодексу України (КПК України) для забезпечення відповідності європейським стандартам.

1. Мінімальні запобіжні заходи та гарантії проти зловживань: практика ЄСПЛ

Практика ЄСПЛ містить значний масив рішень щодо застосування заходів стеження, що зумовлено їхнім специфічним характером. Тоді як відсутність інформації про стеження забезпечує ефективність втручання[1], Суд зазначає, що в таких випадках ризики свавілля є очевидними. Тому критично важливо деталізувати правила щодо обставин та умов здійснення такого стеження[2]. Окрім того, наділення виконавчої влади або суду необмеженими дискреційними повноваженнями суперечило б принципу правовладдя. Отже, закон повинен чітко визначати межі таких повноважень і порядок їх здійснення, щоб забезпечити особі належний захист від свавільного втручання[3].

Саме із цією метою ЄСПЛ розробив низку мінімальних запобіжних заходів (minimum safeguards)[4] та гарантій (adequate and effective guarantees)[5] для аналізу правомірності режиму державного стеження. Оцінюючи їх наявність у законодавстві держави, Суд інтегрував у свій аналіз такі елементи тесту, як легітимність та необхідність втручання[6].

Відповідні запобіжні заходи та гарантії охоплюють:

1) сферу застосування заходів таємного стеження (що охоплює як характер правопорушень, які можуть стати підставою для таємного стеження, так і категорії осіб, за якими воно може бути встановлене);

2) тривалість таких заходів;

3) порядок зберігання, доступу, вивчення, використання, передачі та знищення перехоплених даних;

---

[1] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 287.*

[2] *Iordachi and Others v Moldova App no 25198/02 (ECtHR, 10 February 2009), n. 39; Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 152; Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 229; Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), n. 62.*

[3] *Iordachi and Others v Moldova App no 25198/02 (ECtHR, 10 February 2009), n. 94; Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 152; Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 230.*

[4] *Kruslin v France App no 11801/85 (ECtHR, 24 April 1990), n. 35; Huvig v France App no 11105/84 (ECtHR, 24 April 1990), n. 34; Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 152; Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 231; Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), n. 56.*

[5] *Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 153; Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 232; Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), n. 57.*

[6] *Dragojević v Croatia App no 68955/11 (ECtHR, 15 January 2015), n. 89; Kvasnica v Slovakia App no 72094/01 (ECtHR, 09 June 2009), n. 84; Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 155; Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 236.*

4) дозвіл на стеження;

5) контроль за здійсненням таких заходів;

6) повідомлення про здійснення стеження та доступні засоби правового захисту.

З огляду на ризик того, що система таємного стеження, створена з метою захисту національної безпеки, може під виглядом такого захисту підірвати або навіть знищити демократію, Суд повинен переконатися в наявності належних та ефективних гарантій проти зловживань[7].

1.1. Сфера застосування заходів таємного стеження

Національне законодавство має визначати сферу застосування заходів таємного стеження, чітко окреслюючи характер правопорушень, які можуть стати підставою для стеження, і визначаючи категорії осіб, за якими воно може бути встановлене[8].

1.1.1. Характер правопорушень

Від держав не вимагається наводити вичерпний перелік конкретних правопорушень, однак слід надати достатньо детальну інформацію про їхній характер[9].

Наприклад, у справі *Roman Zakharov v Russia* законодавство дозволяло перехоплення телефонних та інших комунікацій у зв'язку зі злочином середньої тяжкості, тяжким злочином або особливо тяжким кримінальним злочином (злочином, за який передбачається максимальне покарання у вигляді позбавлення волі на строк понад 3 роки), який уже було вчинено, вчиняється або готується. Суд визначив характер злочинів, які можуть стати підставою для ухвалення постанови про прослуховування, достатньо чітким[10]. Проте він також висловив занепокоєння, що прослуховування дозволене стосовно дуже широкого кола кримінальних правопорушень, у тому числі, наприклад, кишенькових крадіжок[11], що також було визнано недоліком у справі *Pietrzak and Bychawska-Siniarska and Others v Poland*[12].

---

[7] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 232; Szabó and Vissy v Hungary App no 37138/14 (ECtHR, 12 January 2016), n. 57.*

[8] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 243.*

[9] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 244; Kennedy v The United Kingdom App no 26839/05 (ECtHR, 18 May 2010), n. 159.*

[10] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 244.*

[11] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 244.*

[12] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 198.*

У справі *Ekimdzhiev and Others v Bulgaria* ЄСПЛ звернув увагу на те, що засоби стеження можуть застосовуватися лише за наявності підстав для підозри, що злочин планується, вчиняється або вже було вчинено і лише якщо інші методи розслідування не дадуть бажаного результату[13].

Щодо стеження з міркувань національної безпеки, то в справі *Roman Zakharov v Russia* Суд зауважив, що законодавство, яке дозволяє перехоплення на підставі інформації про події, що загрожують національній безпеці, без уточнення цих подій, є недостатньо чітким[14].

Водночас у справі *Ekimdzhiev and Others v Bulgaria* ЄСПЛ зазначив, що навіть у разі визнання «захисту національної безпеки» самостійною підставою для стеження, це не суперечитиме Конвенції, якщо потенційним зловживанням можна запобігати в межах незалежного судового контролю[15].

1.1.2. Категорії осіб

Щодо категорій осіб, за якими може бути встановлене стеження, то в справі *Ekimdzhiev and Others v Bulgaria* Суд назвав чітко визначеними такі категорії:

- особи, підозрювані у вчиненні злочинів;
- особи, яких несвідомо використовували для підготовки чи вчинення злочинів;
- особи, які дали згоду на стеження з метою власного захисту;
- свідки, які співпрацюють у справах, пов'язаних з обмеженим колом тяжких умисних злочинів, а також
- об'єкти, що можуть сприяти ідентифікації таких осіб у разі, якщо особи, пов'язані з ними, не встановлені[16].

Суд також констатував правомірність стеження за особою, яка не підозрюється в злочині, але може мати важливу інформацію, проте за умови уточнення практичного застосування таких норм[17].

---

[13] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 299.*

[14] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 246.*

[15] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), nn. 300, 301.*

[16] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 302.*

[17] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 245.*

1.2. *Тривалість заходів таємного стеження*

Законодавство повинно чітко встановлювати строк дії судового дозволу, умови його поновлення та обставини, за яких він підлягає скасуванню[18].

У справі *Roman Zakharov v Russia* Суд визнав чіткими норми про шестимісячний строк санкціонування[19]. У справі *Pietrzak and Bychawska-Siniarska and Others v Poland* — тримісячний строк[20]. Натомість можливість продовження дозволу до двох років у справі *Ekimdzhiev and Others v Bulgaria* викликала в Суду занепокоєння[21].

Щодо процедури продовження. ЄСПЛ схвально оцінив практику, коли суддя продовжує строк лише після повторного розгляду матеріалів (у справі *Roman Zakharov v Russia*)[22] або повного звіту про результати вже проведеного стеження (*Ekimdzhiev and Others v Bulgaria*)[23]. Водночас у справі *Pietrzak and Bychawska-Siniarska and Others v Poland* Суд звернув увагу на обмеження загальної тривалості стеження (не більше ніж 18 місяців)[24].

1.3. *Порядок зберігання, доступу, вивчення, використання, передачі та знищення перехоплених даних*

У справі *Roman Zakharov v Russia* ЄСПЛ позитивно оцінив норми, згідно з якими дані становлять державну таємницю, зберігаються під печаткою, а доступ мають лише уповноважені особи з відповідним допуском. Також було чітко визначено процедуру передачі даних прокуратурі та умови їх використання як доказів у кримінальному провадженні[25].

Натомість у справі *Ekimdzhiev and Others v Bulgaria* ЄСПЛ визначив такі недоліки: відсутність положень про порядок зберігання, необмежене коло осіб із доступом, відсутність гарантій цілісності матеріалів і загальнодоступних правил щодо перевірки «первинного запису» та «похідного носія інформації»[26].

---

[18] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 250; Centrum för rättvisa v Sweden App no 35252/08 (ECtHR, 25 May 2021), n. 331.*

[19] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 251–252.*

[20] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 202.*

[21] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 305.*

[22] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 251–252.*

[23] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 305.*

[24] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 202.*

[25] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 253.*

[26] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 236–237.*

Щодо знищення матеріалів. ЄСПЛ схвалив знищення даних через шість місяців, якщо особі не висунуто обвинувачення[27], проте розкритикував передачу права на знищення винятково спецслужбам без зовнішнього контролю[28], відсутність спеціальних правил щодо знищення отриманих доказів[29], а також доручення процедури знищення посадовим особам державних служб, які здійснюють стеження та не підлягають жодному зовнішньому й незалежному контролю.[30]

Понад те, у справі *Denysyuk and Others v Ukraine* ЄСПЛ розкритикував засекречення записів про знищення без жодного пояснення причин, через що особа, яка перебуває під наглядом, не має можливості перевірити, чи її конфіденційні або нерелевантні дані були насправді видалені[31]. Окрім того, ЄСПЛ неодноразово наголошував на необхідності негайного знищення даних, які більше не стосуються мети, з якою їх отримали[32].

Наостанок, у справі *Denysyuk v Ukraine* недоліком визнано відсутність алгоритму дій при перехопленні конфіденційної розмови адвоката з клієнтом[33].

1.4. Дозвіл на стеження

У межах цього критерію ЄСПЛ оцінює статус органу, що надає дозвіл, обсяг його повноважень і зміст самого документа[34].

1.4.1. Орган, уповноважений надавати дозвіл на стеження

Суд надає перевагу судовим органам. Несудові органи допустимі лише за умови їх повної незалежності від виконавчої влади[35]. До прикладу, у справі *Ekimdzhiev and Others v Bulgaria* дозвіл на стеження міг надавати лише голова компетентного суду або його прямо уповноважений заступник[36].

---

[27] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 254–255.*

[28] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 254, 256.*

[29] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 329.*

[30] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 213.*

[31] *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 109.*

[32] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 211; Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 255.*

[33] *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 111, 113.*

[34] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 257.*

[35] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 258.*

[36] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 308.*

1.4.2. *Обсяг повноважень органу, уповноваженого надавати дозвіл*

Орган, який надає дозвіл, повинен перевіряти наявність обґрунтованої підозри та пропорційність втручання (чи можна досягти мети менш інтрузивними засобами)[37]. Недоліком ЄСПЛ визнав ненадання судді повних матеріалів (зокрема, тактики проведення оперативно-розшукових заходів, даних про інформаторів тощо), що обмежує здатність суду належним чином оцінити ситуацію[38].

1.4.3. *Зміст дозволу на таємне стеження*

У дозволі на таємне стеження має бути чітко вказано конкретну особу, за якою ведеться стеження, або окреме приміщення як об'єкт, щодо якого видано цей дозвіл[39], а також міркування судді для обґрунтування свого рішення[40].

У справі *Roman Zakharov v Russia* Суд указав на відсутність вимог щодо змісту дозволу на прослуховування, що надає органам правопорядку дуже широкі дискреційні повноваження[41]. Так само в справі *Pietrzak and Bychawska-Siniarska and Others v Poland* законодавство не визначало зміст дозволу, а також не у всіх випадках вимагало вказувати підстави для рішення[42].

Окрім того, згідно із законодавством, проаналізованим у справах *Roman Zakharov v Russia, Ekimdzhiev and Others v Bulgaria* та *Denysyuk and Others v Ukraine*, орган, який звертається по дозвіл, також має обґрунтувати свій запит до судді, а суддя може вимагати від нього підтверджувальні матеріали, якщо вони не були додані до клопотання[43].

1.4.4. *Нагальні процедури*

Справа *Roman Zakharov v Russia* стосувалася національного законодавства, що передбачало «процедуру нагальності» — можливість

---

[37] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 260.*

[38] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 261; Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), nn. 206, 209.*

[39] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 264.*

[40] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 207.*

[41] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 265.*

[42] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 207.*

[43] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 259; Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 309; Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 94–95.*

в екстрених випадках здійснювати стеження без попереднього судового дозволу протягом не більше ніж 48 годин. Про кожен такий випадок необхідно повідомити суддю протягом 24 годин із моменту початку. Якщо за 48 годин судовий дозвіл не видано, стеження має бути негайно припинено[44].

ЄСПЛ визначив як недолік відсутність обмежень у застосуванні «процедури нагальності» щодо стеження, яке здійснюється у зв'язку з подіями або діяльністю, що загрожують національній та іншим типам безпеки. До того ж, хоча законодавство вимагає негайного інформування судді про кожен випадок нагального перехоплення, він може лише санкціонувати продовження таких дій. Проте не має повноважень оцінювати, чи нагальність використання процедури була виправданою, або ухвалювати рішення про збереження чи знищення вже отриманих матеріалів[45].

Натомість у справі *Ekimdzhiev and Others v Bulgaria* ЄСПЛ позитивно оцінив застосування цієї процедури, якщо існує безпосередня небезпека вчинення тяжкого умисного злочину або безпосередня загроза національній безпеці. Суддя повинен протягом 24 годин оцінити та ретроспективно затвердити необхідність таких дій, а також уже проведене стеження та його результати або ж операцію потрібно припинити[46].

1.5. Контроль за здійсненням таких заходів

ЄСПЛ напрацював фактори для визначення достатності механізмів нагляду, а саме такі: незалежність органів нагляду, їхня компетенція й повноваження та можливість ефективного громадського контролю за роботою цих органів[47].

1.5.1. Незалежність органів нагляду

ЄСПЛ встановив, що, хоча бажано доручати наглядовий контроль судді, нагляд несудовим органом можливий, якщо він незалежний від органів, які здійснюють стеження, і наділений достатніми повноваженнями та компетенцією для здійснення ефективного та безперервного контролю[48].

---

[44] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 266.*

[45] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 266.*

[46] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 323.*

[47] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 334.*

[48] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 275.*

У справі *Roman Zakharov v Russia* ЄСПЛ мав сумніви щодо незалежності прокурорів, уповноважених здійснювати нагляд від виконавчої влади[49], що зумовлено їхнім призначенням і звільненням Генеральним прокурором після консультацій із регіональними органами виконавчої влади[50].

Так само в справі *Ekimdzhiev and Others v Bulgaria* ЄСПЛ зазначив, що немає гарантії, що всі члени Національного бюро — головного наглядового органу — достатньо незалежні від органів влади, яких вони повинні контролювати, адже після відбуття 5-річного терміну мають право повернутися на попередні посади[51] та перед призначенням на посади повинні пройти перевірку безпеки одним із тих органів, роботу яких вони контролюють[52].

У справі *Pietrzak and Bychawska-Siniarska and Others v Poland* ЄСПЛ постановив, що підпорядкованість прокурорів Головному прокурору Національної прокуратури, ймовірно, загрожує їхній здатності здійснювати незалежний нагляд[53].

1.5.2. Компетенція та повноваження органів нагляду

ЄСПЛ зазначив, що наглядовий орган повинен мати доступ до всіх відповідних документів, зокрема закритих матеріалів, і що всі, хто бере участь у перехопленні, зобов'язані розкривати будь-які потрібні йому матеріали[54].

У справі *Roman Zakharov v Russia* Суд указав на недопустимість виведення тактики й методів спецслужб з-під прокурорського нагляду[55]. Основним недоліком систем у справах *Ekimdzhiev and Others v Bulgaria* та *Pietrzak and Bychawska-Siniarska and Others v Poland* було визнано відсутність у контролерів (прокуратури, бюро чи парламентських комітетів) реальних важелів впливу. Вони не мали повноважень анулювати дозволи, припиняти незаконне стеження або видавати обов'язкові накази про знищення неправомірно отриманих даних[56].

---

[49] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 279–280.*

[50] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 279.*

[51] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 339.*

[52] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 340.*

[53] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 233.*

[54] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 281.*

[55] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), nn. 277, 281.*

[56] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), nn. 343–345; Pietrzak and*

1.5.3. *Можливість ефективного громадського контролю за роботою органів нагляду*

У справі *Roman Zakharov v Russia*, ЄСПЛ зазначив, що, хоч прокурори, які здійснюють нагляд, і повинні були подавати Генеральній прокуратурі піврічні звіти з детальним описом результатів перевірок, ці звіти стосувалися всіх видів оперативно-розшукових заходів, об'єднаних разом, без виокремлення перехоплень. Такі звіти були конфіденційними й недоступними громадськості, при цьому містили лише статистичну інформацію, без уточнення характеру порушень або заходів, вжитих для їх усунення[57].

1.6. *Повідомлення про здійснення стеження та доступні засоби правового захисту*

Ключові фактори — наявність вимоги щодо повідомлення особи про стеження та залежність засобів правового захисту від такого повідомлення[58].

ЄСПЛ визнає, що на практиці не завжди можливо вимагати повідомлення в усіх випадках. Повідомлення кожної особи, на яку поширюється стеження, може поставити під загрозу його довгострокову мету[59]. Однак за відсутності засобів правового захисту, доступних без попереднього повідомлення, воно обов'язкове в усіх випадках, щойно це можна зробити без шкоди для мети здійсненого стеження[60].

У справі *Roman Zakharov v Russia,* зазначено, що осіб, чиї повідомлення прослуховувалися, не інформують про цей факт за жодних обставин[61]. Щоб мати змогу подати запит на інформацію про відповідні дані, в особи мають бути певні відомості про оперативно-розшукові заходи, яким вона піддавалася, а інформація про прослуховування надається лише за дуже обмежених обставин[62].

Так само в справі *Pietrzak and Bychawska-Siniarska and Others v Poland* польське законодавство не передбачало жодного механізму повідомлення особи, окрім випадків, коли проти відповідної особи порушено кримінальне провадження, а перехоплені дані використовуються як докази в провадженні[63].

Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May 2024), n. 234–235.

[57] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 283.*

[58] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 348.*

[59] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 287.*

[60] *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 349.*

[61] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 289.*

[62] *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 290.*

[63] *Pietrzak and Bychawska-Siniarska and Others v Poland App nos 72038/17 and 25237/18 (ECtHR, 28 May*

У справі *Ekimdzhiev and Others v Bulgaria* особі, за якою велося таємне стеження, повідомляється про нього лише у випадку, якщо це відбулося з порушенням закону і стосується тільки фізичних осіб[64].

Натомість у справі *Denysyuk and Others v Ukraine* законодавство вимагає повідомлення суб'єктів стеження протягом 12 місяців після його завершення (або після судового розгляду), що ЄСПЛ розцінив як «*відчутний крок вперед*», але зазначив, що повідомлення ефективне лише тоді, коли супроводжується доступом до фактичних і правових підстав втручання[65].

Щодо **засобів правового захисту**. У справі *Roman Zakharov v Russia* ЄСПЛ дійшов висновку, що скарга до керівника посадовця або прокурора не є ефективним засобом правового захисту, оскільки звернення до безпосереднього керівника органу, дії якого оскаржуються, а також прокурора не відповідає необхідним стандартам незалежності[66]. Натомість засоби правового захисту перед судом доступні лише особам, які мають інформацію про прослуховування їхніх повідомлень. Їхня ефективність підривається відсутністю вимоги про повідомлення суб'єкта прослуховування або належної можливості звернутися до органів влади з проханням надати інформацію про прослуховування та врешті отримати її[67].

У справі *Ekimdzhiev and Others v Bulgaria* засоби правового захисту також були визнані неефективними, оскільки деякі з них не могли бути реалізовані за відсутності попереднього повідомлення, не могли бути використані юридичними особами[68], а також були обмежені грошовим відшкодуванням без можливості судів видавати розпорядження про знищення матеріалів стеження[69].

У справі *Denysyuk and Others v Ukraine* ЄСПЛ визнав, що українське законодавство не має достатніх процесуальних гарантій. Серед недоліків такі:

- неможливість самостійного ініціювати подання скарг відповідно до статей 303 або 309 КПК України[70];

2024), n. 240.

64 *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 349.*

65 *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 120–121.*

66 *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 292.*

67 *Roman Zakharov v Russia App no 47143/06 (ECtHR, 4 December 2015), n. 298.*

68 *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 352.*

69 *Ekimdzhiev and Others v Bulgaria App no 70078/12 (ECtHR, 11 January 2022), n. 353.*

70 *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 126.*

- відсутність у суддів першої інстанції конкретних повноважень перевіряти необхідність стеження або міркування судді, який надав первинний дозвіл (стаття 315 КПК України)[71];

- відмова надати доступ до «секретних» судових рішень[72];

- відсутність дискреційних повноважень, які існували в Кримінально-процесуальному кодексі 1960 року, що дозволяли суддям виносити «окремі рішення» про визнання порушення прав[73] тощо.

2. Вимоги Європейського акта про свободу медіа (EMFA) щодо інтрузивного стеження за журналістами

Регламент (ЄС) 2024/1083, відомий як Європейський акт про свободу медіа (EMFA), встановлює надзвичайно високий стандарт захисту від використання програмного забезпечення для інтрузивного стеження за журналістами.

EMFA визначає подібне програмне забезпечення як продукт, здатний здійснювати несанкціоноване стеження шляхом перехоплення повідомлень, доступу до контенту, активації мікрофона / камери чи збору геолокаційних даних без відома користувача[74].

Так, стаття 4(3)(c) EMFA встановлює, що захисту від інтрузивного стеження підлягають провайдери медіапослуг (медіаорганізації), редакційний персонал та журналісти (зокрема, фрилансери), члени їхніх сімей та особи, які перебувають у регулярних приватних або професійних відносинах із ними (*наприклад*, IT-підтримка, юристи медіа)[75].

Відступ від вимог відповідної статті дозволений за умови дотримання таких кумулятивних вимог[76]:

1. Захід має бути передбачений законодавством ЄС або національним законодавством, а також відповідати статті 52(1) Хартії ЄС, іншим законам ЄС.

2. Захід має бути виправданий у кожному конкретному випадку переважаючим суспільним інтересом та бути пропорційним.

---

[71] *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 127, 129.*

[72] *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 119, 130.*

[73] *Denysyuk and Others v Ukraine App nos 22790/19 and 3 others (ECtHR, 13 February 2025), n. 123.*

[74] *EMFA, Преамбула, п. 25.*

[75] *EMFA, ч. 3 ст. 4.*

[76] *EMFA, ч.ч. 4–5 ст. 4.*

3. Необхідний попередній дозвіл судового органу або незалежного та неупередженого органу (у невідкладних і належним чином обґрунтованих випадках дозвіл можна отримати після застосування заходу «без невиправданої затримки»).

4. Стеження може здійснюватися винятково з метою розслідування в таких категоріях кримінально-протиправних діянь:

   a. Діяння, передбачені статтею 2(2) Рамкового рішення 2002/584/JHA про європейський ордер на арешт, якщо за них передбачено покарання у вигляді позбавлення волі на строк не менше ніж 3 роки[77].

   b. Будь-які інші тяжкі злочини згідно з національним законодавством, якщо за них передбачено покарання у вигляді позбавлення волі на строк не менше ніж 5 років.

3. Рекомендації щодо вдосконалення КПК України для захисту журналістських комунікацій

3.1. Визначення основних термінів Кодексу

Станом на зараз Кримінальний процесуальний кодекс України (КПК) містить положення про «зняття інформації з транспортних телекомунікаційних мереж» (стаття 263) та «зняття інформації з електронних інформаційних систем» (стаття 264). Однак у них не розрізняється звичайне перехоплення трафіку та використання програмного забезпечення для інтрузивного стеження, яке за своєю природою є всеохопним «обшуком» приватного життя особи.

Необхідно доповнити частину 1 статті 3 КПК України таким визначенням поняття «інтрузивне програмне забезпечення для стеження»: «Будь-який програмний продукт, призначений для таємного віддаленого доступу до електронної інформаційної системи або її частин, що дозволяє здійснювати моніторинг дій користувача, перехоплення та читання текстових, аудіо- та відеоповідомлень (зокрема, зашифрованих), отримання геолокаційних даних, а також дистанційну активацію мікрофона або камери пристрою без відома власника».

Окрім цього, варто врахувати, що захист має поширюватися не лише на журналістів, а й на редакторів, працівників редакцій, суб'єктів у сфері

---

[77] *Рамкове Рішення Ради від 13 червня 2002 року про європейський ордер на арешт та процедури передачі правопорушників між державами-членами (2002/584/ЮВС), ч. 2 ст. 2.*

медіа та інших осіб, які через свої професійні обов'язки чи інші регулярні відносини можуть мати інформацію про журналістські джерела.

EMFA також захищає не лише зміст комунікацій, а й інформацію, яка дозволяє встановити джерело. Тому варто забезпечити, щоб гарантії захисту поширювалися на IP-адреси, журнали з'єднань, дані геолокації, білінг та інші комунікаційні метадані.

3.2. Критерії санкціонування НСРД

Необхідно внести зміни до частини 3 статті 248 КПК України, відповідно до яких слідчий повинен довести, що всі інші доступні менш інтрузивні методи були застосовані, однак не дали результату або що вони є очевидно неефективними.

У частину 4 статті 248 КПК України необхідно додати, що ухвала слідчого судді про дозвіл на проведення негласних слідчих (розшукових) дій (НСРД) повинна містити конкретні причини, чому право осіб має бути обмежене в інтересах суспільства в цьому конкретному випадку. Ухвала слідчого судді щодо НСРД, які можуть вплинути на конфіденційність журналістських комунікацій, має містити обґрунтування неможливості досягнення мети менш інтрузивними заходами та оцінку пропорційності втручання.

3.3. Захист конфіденційної інформації

Стаття 258 КПК України передбачає, що ніхто не може зазнавати втручання в приватне спілкування без ухвали слідчого судді. Задля забезпечення конфіденційності «привілейованої інформації», зокрема комунікацій між журналістами та їхніми джерелами, статтю 258 КПК України слід доповнити положенням про те, що якщо в разі проведення НСРД було зафіксовано спілкування особи із журналістом, що стосується виконання ними професійних обов'язків, таке спілкування не може бути використане як доказ у кримінальному провадженні, окрім випадків, коли відповідне втручання прямо було санкціоноване судом із дотриманням спеціальних гарантій, передбачених законом.

3.4. Забезпечення права на оскарження

До статті 253 КПК України варто внести такі зміни:

1. Особу, щодо якої здійснювалися НСРД, потрібно повідомляти про це без невиправданої затримки після припинення відповідних заходів, якщо таке повідомлення більше не створює ризику для досягнення мети кримінального провадження. Також можна розглянути пропозицію

скоротити передбачений граничний строк повідомлення осіб, щодо яких здійснювалося НСРД, з 12 до 6 місяців після припинення таких дій.

2. Разом із таким повідомленням особа повинна отримати копію ухвали слідчого судді про дозвіл на НСРД. Вона має отримувати достатню інформацію для ефективного оскарження законності втручання, у тому числі доступ до інших судових рішень і матеріалів, які можуть бути розкриті без шкоди для законної мети розслідування.

3. Практику «засекречування» ухвал після завершення НСРД потрібно припинити.

У статті 255 КПК України також варто передбачити, що знищення матеріалів НСРД, які не були використані в суді, проводить комісія за участі представника органу адвокатського самоврядування або Уповноваженого Верховної Ради України з прав людини (якщо втручання стосувалося професійних суб'єктів), з метою гарантування повного видалення інформації, що стосується приватного життя особи.

3.5 Особливості правового режиму воєнного стану

Особливий режим кримінального провадження в умовах воєнного стану, передбачений статтею 615 КПК України, дозволяє делегувати повноваження слідчого судді прокурору в разі неможливості виконання судом своїх функцій (пункт 2 частини 1 статті 615).

Відповідну норму варто доповнити положенням про те, що будь-який дозвіл на проведення НСРД, виданий прокурором, має бути поданий на затвердження слідчому судді протягом 72 годин після відновлення роботи суду. У разі незатвердження отримані внаслідок НСРД дані підлягають негайному знищенню, а їх використання як доказу в кримінальному провадженні має бути заборонено.

3.6. Додаткові гарантії

Хоча ця аналітика зосереджена саме на забезпеченні захисту конфіденційних комунікацій при НСРД, журналістські джерела часто розкриваються через тимчасовий доступ до телефонів, серверів, електронної пошти, даних операторів і провайдерів. Тож окремі аналогічні гарантії необхідні для процедур тимчасового доступу (статті 159–166 КПК України). Також варто розглянути зміни щодо запровадження спеціального режиму проведення обшуків у редакціях, медіаорганізаціях і журналістів із підвищеним стандартом обґрунтування та забороною вилучення масивів інформації без попереднього відбору релевантних матеріалів (статті 234–236 КПК України).

ВИСНОВКИ

Сучасне кримінальне процесуальне законодавство України потребує трансформації для відповідності європейським стандартам захисту права на приватність і свободи медіа.

Ключовий висновок полягає в тому, що правомірність таємного стеження залежить не лише від факту наявності судового дозволу, а насамперед від «якості закону», який має бути достатньо чітким, щоб унеможливити будь-яке свавілля виконавчої влади.

Практика ЄСПЛ демонструє, що відсутність деталізованих правил щодо тривалості заходів, порядку зберігання та негайного знищення нерелевантних даних автоматично перетворює систему стеження на інструмент, що загрожує демократичним засадам суспільства.

Особливої ваги набуває питання захисту журналістської діяльності: вимоги Європейського акта про свободу медіа (EMFA) передбачають необхідність доведення переважаючого суспільного інтересу та дотримання жорстких критеріїв щодо тяжкості правопорушень задля інтрузивного стеження за відповідними особами.

Для України це означає необхідність запровадження в Кримінальному процесуальному кодексі України окремого правового режиму для використання програмного забезпечення з метою інтрузивного стеження за журналістами як форми негласних слідчих (розшукових дій). Таке регулювання повинне чітко розмежовувати звичайне зняття інформації з мереж і повний цифровий «обшук» приватного життя, що стає можливим завдяки сучасним технологіям.

The ECtHR was satisfied with a safeguard

The ECtHR was not satisfied with a safeguard

Roman Zakharov v Russia (2015)	
Type of interception	Targeted interception
Abbreviations	OSAA — the Operational-Search Activities Act of 12 August 1995 CCrP — the Code of Criminal Procedure of 18 December 2001
Scope of application of secret surveillance measures	1. Both the OSAA and the CCrP provide that telephone and other communications may be intercepted in connection with an offence of medium severity, a serious offence or an especially serious criminal offence (penalty of more than three years' imprisonment) which has been already committed, is being committed or being plotted. (§ 244) 2. Russian law allows secret interception of communications in respect of a very wide range of criminal offences, including for example, pickpocketing. (§ 244) 3. Interceptions may be ordered not only in respect of a suspect or an accused, but also in respect of a person who may have information about an offence or may have other information relevant to the criminal case. There are no clarifications in legislation or established case-law as to how the terms are to be applied in practice. (§ 245) 4. The OSAA also provides that telephone or other communications may be intercepted following the receipt of information about events or activities endangering Russia's national, military, economic or ecological security. Which events or activities may be considered as endangering such types of security interests is not defined anywhere in Russian law. (§ 246)

The duration of secret surveillance measures	1. Both the CCrP and the OSAA provide that interceptions may be authorised by a judge for a period not exceeding six months. (§ 251) 2. Under both the CCrP and the OSAA a judge may extend interception for a maximum of six months at a time, after a fresh examination of all the relevant materials. (§ 251) 3. The requirement to discontinue interception when no longer necessary is mentioned in the CCrP only. The OSAA does not contain such a requirement. (§ 251) **Overall:** The ECtHR concluded that Russian law contains clear rules on the duration and renewal of interceptions providing adequate safeguards against abuse, however the OSAA provisions on discontinuing surveillance measures do not provide sufficient guarantees against arbitrary interference. (§ 252)
Procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data	1. Russian law stipulates that data collected as a result of secret surveillance measures constitute a State secret and are to be sealed and stored under conditions excluding any risk of unauthorised access. (§ 253) 2. Data collected may be disclosed to those State officials who genuinely need it for the performance of their duties and have the appropriate level of security clearance. (§ 253) 3. Steps must be taken to ensure that only the amount of information needed by the recipient to perform his duties is disclosed, and no more. (§ 253) 4. The official responsible for ensuring that the data are securely stored and inaccessible to those without the necessary security clearance is clearly defined. (§ 253) 5. The law sets out the conditions and procedures for communicating intercepted data containing information about a criminal offence to the prosecuting authorities. It describes, in particular, the requirements for their secure storage and the conditions for their use as evidence in criminal proceedings. (§ 253)

	➡ The ECtHR is satisfied that Russian law contains clear rules governing the storage, use and communication of intercepted data, making it possible to minimise the risk of unauthorised access or disclosure. (§ 253) 6. The intercept material must be destroyed after six months of storage if the person concerned has not been charged with a criminal offence. (§ 254, 255) 7. If the person has been charged with a criminal offence, the trial judge must make a decision, at the end of the criminal proceedings, on the further storage and destruction of the intercept material used in evidence. (§ 254, 256) 8. The lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained. (§ 255)
Authorisation of interceptions	1. Russian law contains an important safeguard against arbitrary or indiscriminate secret surveillance: it dictates that any interception of telephone or other communications must be authorised by a court. (§ 259) 2. The law-enforcement agency seeking authorisation for interception must submit a reasoned request to that effect to a judge, who may require the agency to produce supporting materials. (§ 259) 3. The judge must give reasons for the decision to authorise interceptions. (§ 259) 4. Materials containing information about undercover agents or police informers or about the organisation and tactics of operational-search measures may not be submitted to the judge and are therefore excluded from the court's scope of review. (§ 261) 5. The judges are not instructed, either by the CCrP or by the OSAA, to verify the existence of a "reasonable suspicion" against the person concerned or to apply the "necessity" and "proportionality" test. (§ 262)

6. The CCrP requires that a request for interception authorisation must clearly mention a specific person whose communications are to be intercepted, as well as the duration of the interception measure. (§ 265)

7. The OSAA does not contain any requirements either with regard to the content of the request for interception or to the content of the interception authorisation. (§ 265)

➡ The ECtHR considered that such authorisations grant a very wide discretion to the law-enforcement authorities as to which communications to intercept, and for how long. (§ 265)

urgency procedure

8. In urgent cases it is possible to intercept communications without prior judicial authorisation for up to forty-eight hours. A judge must be informed of any such case within twenty-four hours from the commencement of the interception. If no judicial authorisation has been issued within forty-eight hours, the interception must be stopped immediately. (§ 266)

9. Although in the criminal sphere the OSAA limits recourse to the urgency procedure to cases where there exists an immediate danger that a serious or especially serious offence may be committed, it does not contain any such limitations in respect of secret surveillance in connection with events or activities endangering national, military, economic or ecological security. (§ 266)

10. Although Russian law requires that a judge be immediately informed of each instance of urgent interception, his power is limited to authorising the extension of the interception measure beyond forty-eight hours. He has no power to assess whether the use of the urgent procedure was justified or to decide whether the material obtained during the previous forty-eight hours is to be kept or destroyed. (§ 266)

	➡ Law does not provide for an effective judicial review of the urgency procedure. (§ 266) **Overall:** The ECtHR considered that the authorisation procedures provided for by Russian law are not capable of ensuring that secret surveillance measures are not ordered haphazardly, irregularly or without due and proper consideration. (§ 267) ***the authorities' access to communications*** 11. In Russia the law-enforcement authorities are not required under domestic law to show the judicial authorisation to the communications service provider before obtaining access to a person's communications, except in connection with the monitoring of communications-related data under the CCrP. (§ 269) 12. Indeed, pursuant to Orders issued by the Ministry of Communications, in particular the addendums to Order no. 70, communications service providers must install equipment giving the law-enforcement authorities direct access to all mobile-telephone communications of all users. (§ 269) 13. The communications service providers also have an obligation under Order no. 538 to create databases storing information about all subscribers, and the services provided to them, for three years; the secret services have direct remote access to those databases. (§ 269)
Supervision of the implementation of secret surveillance measures	1. Order no. 70 requires that the equipment installed by the communications service providers not record or log information about interceptions. (§ 272) ➡ It makes impossible for the supervising authority to discover interceptions carried out without proper judicial authorisation. (§ 272) 2. Subsequent supervision is entrusted to the President, Parliament, the government, the Prosecutor General and competent lower-level prosecutors. (§ 274)

	3. Russian law does not set out the manner in which **President, Parliament and the Government** may supervise interceptions. There are no publicly available regulations or instructions describing the scope of their review, the conditions under which it may be carried out, the procedures for reviewing the surveillance measures or for remedying the breaches detected. (§ 276) 4. The law sets out the scope of, and the procedures for, **prosecutors'** supervision of operational-search activities. The prosecutors may carry out routine and *ad hoc* inspections of agencies performing operational-search activities and are entitled to study the relevant documents, including confidential ones; they may take measures to stop or remedy the detected breaches of law and to bring those responsible to account; they must submit biannual reports detailing the results of the inspections to the Prosecutor General's Office. (§ 277) ➡ The ECtHR accepts that there is a legal framework which provides, at least in theory, for some supervision by prosecutors of secret surveillance measures. (§ 277) 5. The prosecutors are appointed and dismissed by the Prosecutor General after consultation with the regional executive authorities. (§ 279) ➡ This fact may raise doubts as to their independence from the executive. (§ 279) 6. Prosecutor's offices do not specialise in supervision of interceptions. It is only one part of their broad and diversified functions, which include prosecution and supervision of criminal investigations. They give approval to all interception requests lodged by investigators in the framework of criminal proceedings. (§ 280) ➡ This blending of functions may also raise doubts as to prosecutors' independence. (§ 280) 7. Russian law stipulates that prosecutors are entitled to study relevant documents, including confidential ones. However, the information about the security services' undercover agents, and about the tactics, methods and means used by them, is outside the scope of prosecutors' supervision. (§ 281)

	8. Interceptions performed by the FSB in the sphere of counter-intelligence may be inspected only following an individual complaint. As individuals are not notified of interceptions, it is unlikely that such a complaint will ever be lodged. (§ 281) 9. The prosecutors have certain powers with respect to the breaches detected by them: they may take measures to stop or remedy the detected breaches of law and to bring those responsible to account. (§ 282) 10. There is no specific provision requiring destruction of the unlawfully obtained intercept material. (§ 282) 11. Prosecutors must submit biannual reports detailing the results of the inspections to the Prosecutor General's Office. However, these reports concern all types of operational-search measures, amalgamated together, without interceptions being treated separately from other measures. (§ 283) 12. The reports contain only statistical information about the number of inspections of operational-search measures carried out and the number of breaches detected, without specifying the nature of the breaches or the measures taken to remedy them. (§ 283) 13. The reports are confidential documents. They are not published or otherwise accessible to the public. (§ 283) **Overall:** The ECtHR considered that the prosecutors' supervision of interceptions as it is currently organised is not capable of providing adequate and effective guarantees against abuse. (§ 285)
Notification of interception of communications and available remedies	1. In Russia persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. (§ 289)

2. A person who has somehow learned that his communications have been intercepted may request information about the corresponding data. In order to be entitled to lodge such a request the person must be in possession of the facts of the operational-search measures to which he was subjected. (§ 290)

3. The interception subject is at best entitled to receive "information" about the collected data, but not to access documents relating to interception of his communications. Such information is provided only in very limited circumstances, namely if the person's guilt has not been proved: that is, he has not been charged or the charges have been dropped on the ground that the alleged offence was not committed; or one or more elements of a criminal offence were missing. (§ 290)

4. Only information that does not contain State secrets may be disclosed to the interception subject while information about the facilities used in operational-search activities, the methods employed, the officials involved and the data collected constitutes a State secret. (§ 290)

➡ In view of the above features of Russian law, the possibility of obtaining information about interceptions appears to be ineffective. (§ 290)

complaint to the official's superior or a prosecutor

5. Russian law provides that a person claiming that his rights have been or are being violated by a State official performing operational-search activities may complain to the official's superior or a prosecutor. (§ 292)

➡ The ECtHR found that hierarchical appeal to a direct supervisor of the authority whose actions are being challenged does not meet the requisite standards of independence. Prosecutors also lack independence and have a limited scope of review. (§ 292)

complaint to the court

6. The Constitutional Court stated that the interception subject had no right to **appeal** against the judicial decision authorising interception of his communications. (§ 294)

7. Domestic law is silent on the possibility of lodging a **cassation appeal**. The ECtHR has serious doubts as to the existence of a right to lodge a cassation appeal against a judicial decision authorising interception of communications. (§ 294)

8. In order to lodge a **supervisory-review complaint** against the judicial decision authorising interception of communications, the person concerned had to be aware that such a decision existed. In the absence of notification of surveillance measures under Russian law, an individual would hardly ever be able to obtain that information. (§ 294)

9. A complaint under Article 125 of the CCrP may be lodged only by a participant to criminal proceedings while a pre-trial investigation is pending, therefore it is available only to persons who have learned of the interception of their communications in the framework of criminal proceedings against them. (§ 295)

10. As regards the **judicial-review complaint under the Judicial Review Act, Chapter 25 of the CCP and the new Code of Administrative Procedure and a civil tort claim under Article 1069 of the Civil Code**, the burden of proof is on the claimant to show that the interception has taken place and that his rights were thereby breached. In the absence of notification or some form of access to official documents relating to the interceptions, such a burden of proof is virtually impossible to satisfy. (§296)

11. The **criminal remedies for abuse of power**, unauthorised collection or dissemination of information about a person's private and family life and breach of citizens' right to privacy of communications are also available only to persons who are capable of submitting to the prosecuting authorities at least some factual information about the interception of their communications. (§297)

Overall: The ECtHR finds that Russian law does not provide for effective remedies to a person who suspects that he has been subjected to secret surveillance.

Centrum för Rättvisa v Sweden (2021)	
Type of interception	Bulk interception
Abbreviations	FRA — *Försvarets radioanstalt* (EN — National Defence Radio Establishment)
The grounds on which bulk interception may be authorised	1. The Signals Intelligence Act restricts bulk interception to exhaustive list of purposes, *i.e.* to monitor: ◆ external military threats to the country; ◆ conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations; ◆ strategic circumstances concerning international terrorism or other serious cross-border crime that may threaten essential national interests; ◆ the development and proliferation of weapons of mass destruction, military equipment and other similar specified products; ◆ serious external threats to society's infrastructure; ◆ foreign conflicts with consequences for international security; ◆ foreign intelligence operations against Swedish interests; and ◆ the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (§ 284). 2. The ECtHR found that the level of detail provided in the legislation and its preparatory works circumscribes the area of bulk interception with "sufficient clarity," even when dealing with evolving foreign threats (§ 285). 3. While the law allows for the monitoring of "serious cross-border crime," this is strictly limited to instances that threaten significant national interests, such as severe drug or human trafficking (§ 286).

	4. A fundamental safeguard exists in the Foreign Intelligence Act, which excludes the use of signals intelligence for traditional law enforcement or operative crime prevention (§§ 286–287). 5. There is a strict prohibition on using any information obtained through signals intelligence as evidence in criminal proceedings (§ 287). 6. Tasking directives (the orders to collect data) may not be issued for the purpose of investigating criminal offenses (§ 287). 7. Although the Security Police and certain police departments may access analysis results, the ECtHR found the Government's clarification that such access is only for strategic assessments, and the ban on investigative use fully applies, as convincing (§ 287). 8. The grounds for authorization are clearly circumscribed, which allows for effective control during the authorization stage and proper *ex post facto* supervision (§ 288). **Overall:** The ECtHR concluded that the grounds for bulk interception in Sweden are clearly defined and sufficiently separated from criminal investigation functions, satisfying the requirement that the law must be clear and predictable (§§ 285, 288).
The circumstances in which an individual's communications may be intercepted	1. For fibre optic cables, signals intelligence is legally restricted to communications crossing the Swedish border. Intercepting communications between a sender and receiver both located in Sweden is prohibited (§ 290). 2. The ECtHR acknowledged the technical reality that separating domestic traffic from foreign traffic is not always possible during the initial stages of interception (§ 290). 3. The FRA is permitted to intercept signals for "development activities" to analyze systems and transmission routes, even if that data does not fall within the eight regular intelligence purposes. The ECtHR found it "satisfactory" and "convincing" because the authorities must be able to adapt to evolving technology and signal protection methods (§§ 291–292).

	4. The degree of interference with privacy rights during development activities is considered to be of a "very low intensity" because the data is used for technological analysis, not for generating intelligence (§ 292). 5. Any information emerging from development activities cannot be used as intelligence unless it conforms to the eight statutory purposes and tasking directives (§ 293). 6. Development activities are not exempt from oversight — they require a permit from the Foreign Intelligence Court and are subject to supervision by the Inspectorate (§ 293). **Overall:** The ECtHR accepted that the Swedish legal provisions on bulk interception define the circumstances in which communications may be intercepted with "sufficient clarity" (§ 294).
The procedure to be followed for granting authorisation	1. Every signals intelligence mission must be authorized in advance by the Foreign Intelligence Court, which acts as a mandatory judicial check (§ 295). 2. In urgent cases, the FRA may grant its own permit, but this triggers an immediate "rapid review" by the court, which has the binding power to modify or revoke it (§ 295). 3. The Foreign Intelligence Court meets the requirement of independence from the executive because its leaders are permanent judges with legally defined terms, and its decisions are immune from Government or Parliamentary interference (§ 296). 4. Although proceedings are confidential and lack public hearings due to secrecy requirements, the mandatory presence of a "privacy protection representative" (a judge or attorney) acts as a relevant safeguard against arbitrariness (§ 297). 5. The FRA is legally required to specify the need for intelligence, the communication bearers, and the specific selectors (or categories of selectors) when applying for a permit (§ 298).

	6. Section 3 of the Signals Intelligence Act creates a binding obligation for selectors to be formulated to limit interference "as far as possible," ensuring a necessity and proportionality analysis at the authorization stage (§ 299). 7. The law provides enhanced protection for "strong selectors" (linked to specific natural persons) by requiring the Foreign Intelligence Court to verify that their use is of "exceptional importance" (§ 300). 8. FRA specifies only "categories" of selectors (§ 301). 9. Swedish system offers a comprehensive ex ante judicial review that is sufficiently detailed to prevent abusive or clearly disproportionate bulk interception (§ 302). **Overall:** The Swedish authorization system provides a significant safeguard through a judicial *ex ante* review that sets a clear legal framework and limits for every interception operation (§ 302).
The procedures to be followed for selecting, examining and using intercept material	1. Interception in Sweden is primarily automated for cable-based signals, while airway signals may be manual. Still, even manual military radio interception is covered by the same legal safeguards as cable communications (§§ 303, 305). 2. The examination process follows a strict progression, *i.e.* automated processing (cryptoanalysis and translation) leads to manual analysis, which then results in a disseminated intelligence report (§ 306). 3. FRA is under a legal obligation to discard intercepted domestic communications immediately upon identification (§ 307). 4. The FRA systematically maintains logs and records of every step, including the selectors used, the time of search, the analyst's name, and the specific tasking directive justifying the search (§ 309). 5. The obligation to keep detailed logs is set out in internal instructions rather than domestic law. But the existence of oversight mechanisms makes it unlikely that these practices would be arbitrarily removed (§ 311).

	6. Under the FRA Personal Data Processing Act, data collection must be adequate, relevant, and limited to what is necessary for the authorized purpose, with a requirement to correct or obliterate incorrect information (§ 312). 7. FRA staff are security cleared, bound by confidentiality, and subject to criminal sanctions for the mismanagement of personal data (§ 312). 8. While personal data protections focus on natural persons, the ECtHR found that legal persons are not left unprotected, as most communications include information related to natural persons and all data remains subject to the original authorized purpose (§§ 314–315). **Overall:** The ECtHR was satisfied that the Swedish legislation regarding the selection, examination, and use of intercepted data provides adequate safeguards against abuse of Article 8 rights (§ 316).
The precautions to be taken when communicating the material to other parties	1. The circle of domestic authorities (such as the Security Police and Armed Forces) that may receive intelligence is narrow, and the regime for sharing results of analysis is clearly circumscribed and low-risk (§ 317). 2. The ECtHR found that the domestic sharing regime does not appear to generate a particular risk of abuse (§ 317). 3. While the law provides for sharing intelligence with foreign partners, the level of generality allows data to be sent whenever it is considered to be in the "national interest" (§ 322). 4. Internal Swedish safeguards (judicial authorization and Inspectorate supervision) that apply when the data is first obtained help limit the risk of adverse consequences after it is transmitted abroad (§ 324). 5. There is a "substantial shortcoming" in the law because it lacks an express requirement for the FRA to assess the necessity and proportionality of intelligence sharing regarding its specific impact on Article 8 privacy rights (§ 326).

	6. The legislation fails to impose a legally binding obligation on the FRA to ensure that a foreign recipient offers an acceptable minimum level of safeguards before data is sent (§ 326). 7. The Government's argument that "shared interest in secrecy" protects data is an insufficient safeguard compared to having clear obligations set out in domestic law (§ 328). 8. Supervisory mechanisms do not sufficiently counterbalance these gaps because the Inspectorate cannot effectively monitor privacy risks if the law doesn't explicitly require the FRA to consider them (§ 329). 9. The absence of a requirement to consider the privacy interests of the individual when making a decision about intelligence sharing is a significant shortcoming of the Swedish regime (§ 330). **Overall:** Regarding the communication of data to foreign partners, the ECtHR found that the Swedish regulatory framework contains significant shortcomings that are not sufficiently counterbalanced by supervisory elements (§§ 329, 330).
The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed	1. Under Section 5(a) of the Signals Intelligence Act, permits are granted for a maximum of six months, and any extension requires a new full examination of conditions by the Foreign Intelligence Court (§ 332). Swedish law provides a "clear indication" of the expiry period and the specific conditions under which a permit may be renewed (§ 332). 2. There is no express provision obliging the intelligence agency (*i.e.* FRA) or the Foreign Intelligence Court to cancel a mission if the conditions for it have ceased to exist or if the measures are no longer necessary (§ 333). ECtHR agreed that an express provision for discontinuation would have been "clearer" than the existing arrangement (§335).

	NB: This was identified as not a fatal shortcoming in the legislative drafting (§§ 335–336). 3. Swedish law provides other "relevant mechanisms" to address necessity, such as the ability of the requesting authority to revoke a tasking directive and the supervision by the Inspectorate (§ 336). The existence of supervision mechanisms with access to all internal information provides "similar legislative safeguards against abuse" regarding the duration of operations (§ 336). 4. Intelligence must be destroyed immediately if it concerns (§ 338): ◆ anonymous authors or media sources (media privilege), attorney-client privilege, religious confessions or individual counseling; ◆ information concerning a specific natural person that is determined to lack importance for the intelligence mission must be destroyed; ◆ if both the sender and receiver are in Sweden, the data must be destroyed as soon as its domestic nature becomes evident; ◆ also, all intelligence collected under a temporary permit that is subsequently revoked by the court must be destroyed immediately. 5. The FRA may maintain databases for raw material containing personal data for up to one year. The ECtHR accepted this as necessary for the processing of signals intelligence. But it stressed that such data should be deleted "as soon as it is evident that it lacks pertinence" (§ 338). 6. The Inspectorate's powers include monitoring the FRA's actual practices regarding the destruction of material what was characterized as an "important safeguard" for the proper application of existing rules (§ 340). 7. The limits on storage and destruction apply primarily to personal data. The law lacks a general rule governing the destruction of other types of material (*e.g.,* data belonging to legal persons/corporations) which still impacts the right to respect for correspondence under Article 8 (§§ 341–342).

	8. There is no explicit legal requirement to delete intercepted data simply because it has lost pertinence for the mission unless it falls into the specific categories mentioned before (§342) 9. The ECtHR noted a lack of information on whether the necessity of continued storage is regularly reviewed during that one-year period, rather than simply keeping all data for the maximum duration by default (§ 343). **Overall:** Swedish law satisfies the requirements concerning the duration of bulk interception of communications (§§ 337, 344).
Supervision	1. Oversight of foreign intelligence is primarily entrusted to the Foreign Intelligence Inspectorate, with additional (though more limited) supervisory functions performed by the Data Protection Authority (§ 345). The Inspectorate is verified as an independent control mechanism with a board presided over by judges, and the members proposed by parliamentary groups rather than being solely executive appointees (§ 346). 2. The Inspectorate possesses wide-ranging powers to oversee the entire intelligence cycle, including the authority to grant or deny access to communication bearers based on court-issued permits, a right to scrutinize all FRA documents, including a specific mandate to examine the selectors used for intercepting data (§ 347). 3. The Inspectorate is capable of assessing not just "formal" lawfulness, but also the proportionality of the interference with individual rights (§ 348). 4. Under Section 10 of the Signals Intelligence Act, the Inspectorate holds the power to issue legally binding decisions to stop improper data collection or order the destruction of recordings (§ 350). 5. While some of the Inspectorate's findings take the form of non-binding "opinions," evidence from the National Audit Office confirms that the FRA treats these suggestions as serious and typically implements requested reforms (§§ 350–351).

	6. The Inspectorate's effectiveness is demonstrated in practice through frequent, themed inspections (102 inspections over 8 years) covering sensitive areas like data destruction and international cooperation (§ 351). 7. Transparency is ensured through the publication of annual reports available to the public and regular audits by the National Audit Office (§ 352). **Overall:** Swedish law provides effective supervision of signals intelligence and entails the judicial pre-authorization procedure (§ 353).
***Ex post facto* review**	1. In practice, no individual is ever notified when their communications have been intercepted, even when "strong selectors" directly related to them are used, due to the secrecy inherent in foreign intelligence (§ 354). The ECtHR accepts the lack of notification as "legitimate" in the context of bulk interception, provided it is counterbalanced by other effective remedies available to individuals (§ 355). 2. Any individual or legal person, regardless of nationality, has the right to request that the Inspectorate investigate whether their communications were unlawfully intercepted, without needing to prove they were actually affected (§ 356). 3. During a review, the Inspectorate has the binding power to stop an operation or order the destruction of data if it finds the law has been breached (§ 356). 4. The Inspectorate only informs the complainant that an investigation was "carried out", but does not confirm if interception occurred or provide a reasoned decision (§§ 357, 361). 5. The Inspectorate supervises and authorizes the FRA's operations what may lead to the assessment of its own activities when reviewing a complaint (§ 359). 6. While the National Audit Office audits the Inspectorate, there is no legal obligation for these audits to regularly cover the specific handling of individual complaints, which weakens this safeguard (§ 360).

	7. The absence of reasoned decisions, even for security-cleared counsel prevents the development of public legal guidance and fails to provide "public confidence" that abuses will be remedied (§ 361). 8. The Parliamentary Ombudsmen and Chancellor of Justice can investigate lawfulness, but do not offer the "adversarial process" or the reasoned decisions necessary for an effective ex post facto review (§ 362). **Overall:** The ECtHR found that Inspectorate's 'dual role' (*i.e.* supervising and then reviewing its own supervision) and the lack of reasoned decisions for complainants fail to meet the requirements of an effective remedy under Article 8 (§ 364).

Big Brother Watch and Others v the United Kingdom (2021)	
Type of interception	Bulk interception
Abbreviations	RIPA — Regulation of Investigatory Powers Act 2000 IC Code — Interception of Communications Code of Practice IC Commissioner — Interception of Communications Commissioner IPT — Investigatory Powers Tribunal
The grounds on which bulk interception may be authorised	1. The Secretary of State can only issue a bulk interception warrant if it is "necessary" for one of three statutory purposes: national security, preventing/detecting serious crime, or safeguarding the UK's economic well-being (provided it is also relevant to national security) (§ 368). 2. The term "national security" is clarified through the IC Code to include protecting the State from activities intended to undermine or overthrow parliamentary democracy by political or violent means (§ 369).

	3. "Serious crime" is strictly defined in Section 81(2)(b) of RIPA based on sentencing thresholds (at least three years imprisonment) or specific conduct like violence and substantial financial gain (§ 369). 4. Similar to the Swedish case, under Section 17 of RIPA intercepted material cannot be used as evidence in legal proceedings or criminal prosecutions (§ 369). 5. Bulk warrants are typically aligned with specific "intelligence priorities" set by the National Security Council, providing an extra-legal layer of strategic targeting (§ 369). **Overall:** The ECtHR held that while the UK's statutory grounds for bulk interception are formulated in "relatively broad terms," they are sufficiently focused to proceed to an assessment of the rest of the system's safeguards (§§ 370–371).
The circumstances in which an individual's communications may be intercepted	1. Section 8(4) warrants target communication "bearers" (the physical or logical data links) rather than specific individuals or premises, allowing for the interception of all data packets flowing through a targeted link (§ 372). 2. Intercepting agencies must use technical surveys and knowledge of international routing to identify and prioritize links most likely to contain "external communications" of intelligence interest (§ 373). 3. A communication is classified as "external" based solely on whether the sender or recipient is outside the British Islands. Notably, a UK-to-UK message remains "internal" even if the data packets physically route through a third country (§ 374). 4. Section 5(6) of RIPA explicitly authorizes the "by-catch" of internal communications if it is a necessary byproduct of intercepting the authorized external material, including cloud storage, browsing history, and social media activities (§ 375). 5. Although broad, the "external communications" distinction acts as a "macro-level" safeguard by circumscribing the categories of people likely to be intercepted based on the specific international gateways chosen for monitoring (§ 375).

	Overall: The ECtHR accepted that the Section 8(4) regime was sufficiently "foreseeable" for Article 8 purposes. Since users cannot control the routing of their data, further legal restrictions on the choice of bearers would not have made the law's effects any more predictable for the individual (§ 376).
The procedure to be followed for granting authorisation	1. Bulk interception warrants are authorized by the Secretary of State following internal agency review what lacks authorization by a body independent of the executive (§ 377). 2. To issue a warrant, the Secretary of State must be satisfied of its necessity and proportionality, requiring a detailed application that explains why the information cannot be obtained through less intrusive methods (§§ 378–379). 3. While specific bearers are not named in the warrant to avoid "serious impracticalities," the application must describe the "sorts of bearers" to be targeted to allow for a proper assessment of the operation's scope (§ 380). 4. Specific search selectors are not included in the warrant. Analysts must record a written justification for each new selector, which is later subject to independent audit and oversight by the IC Commissioner (§ 381). **NB:** The ECtHR ruled that selector categories should be identified at the authorization stage. The UK law does not provide prior internal authorization or objective verification for "strong selectors" linked to specific individuals (§§ 382–383). **Overall:** Section 8(4) was legally deficient because the authorization process was entirely executive-led and lacked prior independent oversight regarding the categories and individual-specific search terms used to filter intercepted data (§§ 377, 383).
The procedures to be followed for selecting, examining, and using intercept material	1. High-volume communications are filtered using "strong selectors" and complex queries to create a searchable index. Under Section 16(2) of RIPA, selectors cannot be used to target an individual known to be in the British Islands unless the Secretary of State personally authorizes it based on necessity and proportionality (§ 384).

	2. Human examination is strictly limited to material on the index that falls within the scope of a "certificate" issued by the Secretary of State. Analysts must provide a written justification for accessing any specific communication, explaining why it is necessary and why the information cannot be obtained through less intrusive means (§ 385). 3. The Court identified a deficiency in the use of these "certificates," noting that they were often drafted in overly general terms (*e.g.* intelligence on terrorism). This lack of precision, combined with the failure to identify selector categories at the warrant stage, meant the certificates provided insufficient restrictions on what material could be examined (§§ 386–387). 4. Procedural safeguards for analysts include a requirement to account for "collateral infringement" of privacy, strict time limits on data access, and regular audits to ensure that the material being examined matches the justifications provided (§ 388). 5. Data management is governed by strict security protocols, *e.g.* only vetted and trained analysts have access, copying is limited by a "need to know" principle, and all material must be stored securely and destroyed when no longer required (§§ 389–390). **Overall:** Despite specific deficiencies regarding the vague nature of the Secretary of State's certificates and the lack of oversight for selector categories, the ECtHR found that the rules governing the selection, examination, and storage of intercepted material were sufficiently "foreseeable" and provided adequate safeguards against abuse (§ 391).
The precautions to be taken when communicating the material to other parties	1. Section 15(2) of RIPA mandates that the disclosure, copying, and distribution of intercepted material must be limited to the "minimum necessary" for specific authorized purposes, such as national security or preventing serious crime (§ 392). 2. The "need-to-know" principle strictly prohibits the disclosure of material to any internal or external person unless their specific duties require that information. Even then, only the specific portion of data necessary for their task can be shared, and all recipients must be appropriately security-vetted (§ 393).

	3. Although the law includes the broad term "likely to become necessary" regarding data retention and sharing, the core requirements for security clearance and "need-to-know" justifications still remained in place (§ 394). 4. When transferring data to foreign intelligence partners (*e.g.* the "Five Eyes"), the UK must take reasonable steps to ensure the partner has adequate procedures for secure storage and limited distribution. Material cannot be shared with a third country without explicit UK consent and must be destroyed when no longer needed (§§ 395–396). 5. Specific safeguards exist for confidential material, requiring it to be clearly marked and necessitating legal advice before dissemination. Furthermore, intercepted material is generally prohibited from being used as evidence in legal proceedings (§§ 392, 397). **Overall:** The precautions governing the communication of intercepted material to other parties were sufficiently clear and provided robust guarantees against abuse, particularly given the added weight of oversight by the IC Commissioner and the Investigatory Powers Tribunal (§§ 398–399).
The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased or destroyed	1. Warrants for national security or economic well-being last for six months, while those issued for serious crime last for three months. Both categories are renewable by the Secretary of State only if the agency provides a fresh assessment proving the continued necessity and proportionality of the interception (§ 400). 2. Agencies must establish maximum retention periods for intercepted material. Typically it is capped at two years and approved by the IC Commissioner with a requirement for automated deletion once these limits are reached (§ 402). 3. In practice, data retention is significantly shorter than the legal maximum. Communications that do not match search criteria are discarded immediately or within a few days, while material selected for human examination is usually deleted after a few months unless it is cited in a formal intelligence report (§ 403).

	4. Continuous review is mandatory to ensure that any retained material still meets statutory necessity grounds. If it no longer does, the warrant must be cancelled and all copies, extracts, and summaries of the data must be securely destroyed (§§ 400, 404). **Overall:** The ECtHR held that the rules regarding the duration and destruction of intercepted material under the Section 8(4) regime were sufficiently clear and provided adequate safeguards. But it still stipulated that the actual, shorter retention practices should be more explicitly reflected in the law and not in the internal policy (§§ 401, 405).
Supervision	1. Pre-authorization scrutiny is conducted by internal agency staff and lawyers to ensure necessity and proportionality before warrants ever reach the Secretary of State for a signature (§ 406). 2. The IC Commissioner, an independent judicial figure, provides external oversight by reviewing the use of RIPA powers, conducting inspections, and reporting findings to the Prime Minister and Parliament (§ 407). It involves a three-stage inspection process: sampling warrants based on sensitivity, performing detailed documentation reviews, including checking the written justifications for every selector used, and interviewing operational or legal staff (§ 410). 3. Supervision extends to international data-sharing agreements, ensuring that foreign partners ("Five Eyes") access UK-intercepted material only through controlled systems that adhere to domestic legal safeguards and staff training standards (§ 411). **Overall:** The IC Commissioner provided independent and effective supervision of the Section 8(4) regime, given the Commissioner's ability to audit a vast volume of warrants, investigate the use of search selectors, and mandate formal improvements through a recommendation-and-report-back system (§ 412).

Ex post facto review	1. The IPT serves as a specialized judicial body, presided over by High Court Judges or senior lawyers, to provide a remedy for those challenging specific surveillance acts or the legality of entire regimes. IPT does not require a person to be notified of interception, anyone who suspects they have been subject to secret surveillance can bring a claim (§ 413). 2. The IPT has full access to all relevant information, including "below the waterline" classified documents that cannot be made public for national security reasons (§ 413). 3. The IPT can award compensation, quash or cancel warrants, and order the secure destruction of any intercepted records (§ 413). 4. The IPT can hold public oral hearings, appoint special counsel to represent claimants in closed proceedings, and publish its legal rulings on a dedicated website (§ 413). **Overall:** The IPT provides a robust judicial remedy for anyone suspecting their communications were intercepted (§ 415).

Ekimdzhiev and Others v Bulgaria (2022)	
Type of interception	Targeted interception
Grounds on which secret surveillance may be resorted to and persons who can be placed under surveillance	1. The law sets outs in an exhaustive manner the serious intentional criminal offences which can trigger the use of special means of surveillance. (§ 299) 2. The law specifies that such means can be used only if there are grounds to suspect that such an offence is being planned, or is being or has been committed, and only if other methods of detection or investigation would be unlikely to succeed. (§ 299)

➡ Although the types of offences falling into that list are varied, in practice in the vast majority of cases the authorities resort to surveillance in relation to the offences of (a) being the leader or member of a criminal gang and of (b) dealing in narcotic drugs.

3. The law stipulates that special means of surveillance can also be used for "activities relating to national security". In the absence of more detailed information about the practice of the relevant courts and authorities, it is difficult to check whether, national security can be a standalone ground for surveillance. However, even if it can, potential abuses can be checked through judicial authorisation for the surveillance. (§ 300, 301)

4. The law also sets out in an exhaustive manner the categories of persons who, or objects which, may be placed under surveillance. (§ 302)

5. When it comes to surveillance relating to criminal offences, the relevant categories are clearly defined: those are either people suspected of committing offences, people unwittingly used for their preparation or commission, people who have agreed to surveillance for their own protection, or cooperating witnesses in cases relating to a limited class of serious intentional offences, as well as objects capable of leading to the identification of such persons if their identity is unknown. (§ 302)

6. When it comes to surveillance on national-security grounds, the law is couched in vaguer terms: "persons or objects related to national security", however potential abuses can be checked through judicial authorisation for the surveillance. (§ 302)

7. The lack of sufficient precision about the meaning of the term "objects" in section 12(1) of the 1997 Act. The Act does not clarify whether the "objects" which may be placed under surveillance need to be concrete (for instance, specific premises, a specific vehicle, or a specific telephone line). (§ 303)

	Overall: Bulgarian law complies with the requirements of Article 8 of the Convention in respect of the grounds on which secret surveillance may be resorted to and persons who can be placed under surveillance, except for the lack of a more precise definition of the term "objects" in section 12(1) of the 1997 Act. (§ 304)
Duration of secret surveillance measures	1. Bulgarian law lays down clearly the initial and maximum duration of secret surveillance measures. (§ 305) 2. Surveillance beyond the initially authorised period is only possible if authorised by the competent judge, who must be presented not only with the same information as that required for the initial authorisation, but also with a full account of any surveillance results obtained so far. (§ 305) 3. The law sets out the circumstances in which surveillance must be stopped. (§ 305) 4. One area of concern is the potential duration of the initial authorisation for surveillance on national-security grounds, which is up to two years. (§ 305) ➡ The sheer length of that period, coupled with the inherently unclear contours of the notion of national security, significantly weakens the judicial control to which such surveillance must be subjected. (§ 305)
Procedures for storing, accessing, examining, using, communicating and destroying surveillance data	1. While the law specifies the way in which information from the "primary recording" is to be reproduced in the "derivative data carrier" and then in any evidentiary material, they say nothing about the way in which they are to be stored. (§ 326) 2. The law does not circumscribe in any way the officials within the relevant authorities who are entitled to access them, or lay down any safeguards ensuring the integrity and confidentiality of those materials. (§ 326)

3. Aside from the general rule that the content of the "derivative data carrier" must fully match that of the "primary recording", no publicly available rules exist on how they are to be examined: how the authorities are to sift through the information in them and decide which parts are relevant and are to be kept and used as evidence, and which parts are irrelevant and are to be discarded. (§ 327)

4. Although the rules governing the possible use of materials obtained as a result of surveillance say that any such materials, including surplus information, can be used only to prevent, detect or prove serious intentional criminal offences, or to protect national security, it is thus unclear how compliance with that limitation is ensured in practice. (§ 327)

5. The rules governing the destruction of the "primary recording" and the "derivative data carrier" appear sufficiently clear, although a discrepancy exists between the position in relation to materials obtained as a result of surveillance outside already pending criminal proceedings and the position in relation to materials obtained in the course of criminal proceedings: the law provides for automatic destruction and subsequent report to the judge who has authorised the surveillance in the former case, and for a report to that judge and destruction by his or her order in the latter case. (§ 328)

6. There is no special rules about the storage or destruction of the resulting evidentiary material. It appears that both copies produced in each case are stored and destroyed together with the case files of which they form part (§ 329)

7. There are no publicly available rules governing the storage of information obtained through surveillance on national-security grounds — which must be kept by the relevant requesting authority for fifteen years after the end of the surveillance. (§ 330)

Overall: The apparent lack of clear regulation in all these fields, and of proper safeguards, makes it possible for information obtained as a result of secret surveillance to be misused for ends which have little to do with the statutory purpose. (§ 332)

	with regard to surveillance affecting legal professional privilege 8. Apart from Chief Prosecutor's instruction on the point, which was a purely internal act, there are no legal provisions, specifying with an appropriate degree of precision the fate of information resulting from secret surveillance which may have affected materials subject to legal professional privilege. (§ 333) 9. The instruction simply makes secret surveillance directed against lawyers subject to the existence of a reasonable suspicion that they have committed an offence, which is in principle a requirement for all surveillance. (§ 333) 10. The instruction seems to contradict the express terms of section 33(1), (2) and (3) of the Bar Act 2004, according to which all lawyers' records and communications, regardless of their form, are privileged without exception. (§ 333) 11. The instruction does not lay down enough safeguards with respect to materials obtained as a result of accidentally intercepted lawyer-client communications. Point 13 says that if the authorities intercept the conversation of a lawyer with a client or with another lawyer, and that conversation touches upon a client's defence, they must not prepare evidentiary material on its basis, unless the surveillance reveals that the lawyer has him- or herself engaged in criminal activity. The question on how precisely any such intercept materials are to be destroyed, as expressly required by section 33(3) of the Bar Act 2004, is open. (§ 333) 12. The instruction does not encompass all sorts of lawyer-client communications: point 13 applies solely to communications relating to a client's defence, which implies already pending litigation, and perhaps even just criminal proceedings. (§ 333)
Authorisation procedures	1. Only a limited number of authorities can request surveillance, within the spheres of their respective competencies. (§ 308)

	2. The law provides for a form of internal review preceding the submission of surveillance applications: those made by executive authorities must originate from the head of the respective authority, and public prosecutors intending to make such applications must notify their hierarchical superiors. (§ 308) 3. Surveillance may be authorised only by the competent court president or an expressly authorised deputy. (§ 308) 4. The authority which carries out the surveillance must, before proceeding with it, scrutinise the surveillance application for incompatibility *ratione materiae* or obvious mistakes and, if it spots issues in those respects, refer the application back to the judge who authorised the surveillance for reconsideration. (§ 308) 5. Surveillance applications must be duly reasoned and set out both the grounds for the requested surveillance and its intended parameters. An application must, in particular: (a) refer to the circumstances giving cause to suspect that a relevant offence is being prepared or committed or has been committed (including when it comes to national security), (b) set out (except in relation to terrorist offences) the investigative steps already taken and the results of any previous inquiries or investigations, (c) explain (except in relation to terrorist offences) why the requisite intelligence cannot be obtained through other means or why such other means would entail exceptional difficulties, and (d) explain (except in relation to terrorist offences) why the intended duration of the surveillance is necessary. (§ 309) 6. All materials on which the application is based must either be enclosed with it from the outset (for applications made outside criminal proceedings), or made available to the competent judge upon request (for applications made in the course of criminal proceedings. (§ 309)

	7. When examining the application, the judge must review whether all legal prerequisites are in place and rule by means of a reasoned decision. (§ 309) 8. One possible shortcoming is that although surveillance-warrant proceedings must of necessity be conducted without notice to the persons intended to be placed under surveillance, the requesting authority is under no duty to disclose to the judge fully and frankly all matters relevant to the well-foundedness of its surveillance application, including matters which may weaken its case. (§ 309) 9. The additional vetting carried out by the surveillance authorities after the grant of judicial authorisation cannot remedy that lack of proper judicial scrutiny since vetting is limited to incompatibility *ratione materiae* or obvious mistakes and the instances in which that additional safeguard has been triggered are apparently extremely rare. (§ 322) ***urgent procedure*** 10. Special means of surveillance may be deployed without a prior judicial warrant if there is an immediate risk that a serious intentional offence is about to be committed, or a risk of an immediate threat to national security. (§ 323) 11. When the authorities resort to that urgent procedure, the competent judge must within twenty-four hours assess and approve retrospectively the need for them to have done so; otherwise the surveillance operation must stop. (§ 323) 12. The judge is not required to just review the need to pursue the surveillance, but must also validate the surveillance which has already taken place, as well as its results. (§ 323)
Oversight arrangements	***National Bureau*** 1. There is no guarantee that all of the members of the **National Bureau**, the main supervisory body, are sufficiently independent *vis-à-vis* the authorities which they must oversee. By law, individuals with professional experience in the law-enforcement or the security services may become the members. After serving their five-year term, they are entitled to regain their previous posts. (§ 339)

➡ This potential "revolving door" mechanism can raise misgivings about the practical independence of such members of the Bureau and about possible conflicts of interests on their part. (§ 339)

2. Before being appointed to their posts, its members must undergo security vetting by one of the very authorities whose work the Bureau is overseeing — the State Agency for National Security. If it later revokes the security clearance of members of the Bureau, they must be removed from their post since they automatically. (§ 340)

➡ Although the Agency's decision to revoke a security clearance is amenable to judicial review, that possibility for it to influence the Bureau's membership is capable of affecting the Bureau's independence and objectivity. (§ 340)

3. Misgivings arise about the qualifications of some of the members of the National Bureau. Only one of its current five members has legal training and experience. (§ 342)

4. It does not appear that when carrying out on-site inspections National Bureau members and employees are able to have unfettered access to all relevant materials held by the prosecuting authorities and the State Agency for National Security, especially materials enabling them to check the well-foundedness of surveillance applications (reasonable suspicion and proportionality in each case). (§ 343)

5. The National Bureau has no power to order remedial measures, such as the destruction of surveillance materials. It can only bring irregularities to the attention of the heads of the relevant authorities and the prosecuting authorities, or of the Supreme Judicial Council, for irregularities attributable to judges. (§ 344)

6. The National Bureau's power to give instructions appears to relate solely to instructions intended to improve practices rather than instructions in specific cases, as attested in particular by their limited number per year. (§ 344)

	special parliamentary committee 7. The **special parliamentary committee** is not empowered to order remedial measures either. It does not appear to conduct regular inspections. (§ 345) **Overall:** The current system of overseeing secret surveillance in Bulgaria does not appear capable of providing effective guarantees against abusive surveillance. (§ 347)
Notification	1. The National Bureau must notify someone who has been placed under secret surveillance only if that has happened unlawfully. (§ 349) ➡ under the ECtHR's case-law such notification is, in the absence of a remedy available without prior notification, required in all cases, as soon as it can be made without jeopardising the purpose of the surveillance. (§ 349) 2. The National Bureau is only required to notify individuals, not legal persons. (§ 349)
Remedies	1. A claim for damages under section 2(1)(7) of the 1988 Act, although effective in some scenarios, has so far not been able to operate in the absence of prior notification by the National Bureau that someone has been placed under surveillance. (§ 352) 2. A claim under the 1988 Act does not entail an examination of the necessity for the surveillance in each case. (§ 352) 3. A claim under the 1988 Act is not open to legal persons. (§ 352) 4. The only form of relief available in the proceedings under the 1988 Act is money damages. The courts have no power to order the destruction of surveillance material. (§ 353) 5. The remedies available under the 2002 Act have so far not been shown to be effective in relation to secret surveillance, and are not available to legal persons. (§ 354)

	Overall: Bulgarian law does not provide an effective remedy to all persons suspecting, without concrete proof, that they have been unjustifiably subjected to secret surveillance. (§ 355)

Pietrzak and Bychawska-Siniarska and Others v Poland (2024)	
Type of interception	Targeted interception
Abbreviations	NIK — *la Chambre suprême de contrôle* (EN — Supreme Chamber of Control)
Scope of covert surveillance measures	1. The law on the national police sets out a list of offences which may give rise to the carrying out of covert surveillance, however it authorises surveillance for a very wide range of criminal offences, including relatively minor offences. (§ 198) 2. The lists of offences for which operational surveillance may be carried out have been specified by the legislature using various legislative techniques. However, very general wording has been used, to the extent that the cases in which the authorities could in practice resort to such a measure could give rise to confusion. (§ 199) 3. The categories of persons liable to be subject to operational surveillance were not specified in the law, so that it could be any individual or group provided that useful information could likely be obtained in this way in view of the purpose of the surveillance. (§ 201) 4. The applications for authorisation to carry out operational surveillance must specify the person targeted by the surveillance in question, which implies that surveillance of this type is always targeted. (§ 201) 5. The legislation does not impose any requirements regarding the content of the decision authorising the surveillance. (§ 201)

The duration of covert surveillance measures	1. A judge may authorise an interception measure for a period not exceeding three months. (§ 202) 2. An extension is possible, subject to a court order, for a further period of up to three months, provided that the original grounds for ordering the surveillance remain valid. In duly justified cases, the surveillance may be extended by a higher court for several consecutive periods, subject to a total limit of twelve months. The surveillance must not last for more than eighteen months in total. (§ 202) 3. The operational surveillance must cease as soon as the reasons justifying its implementation no longer exist and, at the latest, upon the expiry of the period for which it was authorised. (§ 202) **Overall:** The ECtHR considered that domestic law clearly specifies the maximum period at the end of which an interception authorisation expires and the circumstances in which such authorisation may be renewed. It observes that the duration of an interception operation may depend on several factors, however, in view of the shortcomings identified further in the model of covert surveillance, there is no need to examine this issue. (§ 202)
Procedures to be followed regarding the storage, access, examination, use, disclosure and destruction of intercepted data	1. The laws governing the implementation of operational surveillance by various police and intelligence services provide for a framework for the destruction of information gathered through such surveillance which proves to be unnecessary for the achievement of the objectives pursued by the relevant State service. (§ 211) 2. Under the Police Act, information gathered through covert surveillance which is unnecessary for the purposes of such surveillance or which is irrelevant to criminal proceedings must be destroyed without delay by a formal committee. A similar obligation is provided for in cases deemed urgent where retrospective authorisation has not been granted. (§ 211)

	3. The evidence enabling the initiation of criminal proceedings or which is useful to proceedings currently under investigation is forwarded by the competent officials to the public prosecutor. (§ 211) 4. The transmission of evidence gathered by the State services carrying out the operational surveillance to the public prosecutors and the competent courts is carried out in accordance with the provisions applicable to classified information. (§ 212) 5. The State services carrying out covert surveillance are required to maintain electronic records of documents relating to such surveillance. (§ 212) **Overall:** The provisions relating to the processing and destruction of information intercepted by means of operational surveillance set out safeguards for the protection of the data thus collected. (§ 213) 6. The destruction of the data collected is entrusted to officials of the State services carrying out the surveillance and the implementation of this measure is not subject to any external and independent scrutiny of the State services concerned. (§ 213)
Authorisation for interception	1. Only a limited number of authorities may request surveillance within the scope of their respective powers. (§ 204) 2. The law provides for a form of internal control prior to the submission of surveillance requests, which must originate from the head of the relevant law enforcement authority and be approved in advance by the competent prosecutor. (§ 204) 3. The law specifies the content of a request for authorisation of surveillance and requires that it be substantiated. (§ 204) 4. The law requires that operational surveillance be authorised in advance by a judge. (§ 204)

	5. Exceptionally, in cases of urgency, the police may carry out surveillance without such authorisation, but must cease it if they do not obtain such authorisation within five days of the measure being put in place, and all information gathered in this context must then be destroyed. (§ 204) 6. A significant shortcoming is that it does not appear that the legislation requires the judge ruling on the surveillance authorisation to verify the existence of such evidence in respect of the person concerned. (§ 206) 7. The legislation does not specify the content of the interception authorisation nor does it require the court issuing such an authorisation to state the reasons for its decision, except where the decision is unfavourable to the law enforcement agency seeking it. (§ 207) 8. The procedure for authorising covert surveillance lacks any adversarial element. (§ 207) 9. The application of the emergency authorisation procedure is justified solely by the risk of loss of evidence, and not by the seriousness or nature of the offence, leaving the authorities considerable discretion to determine in which situations it is justified to resort to such non-judicial procedure and giving rise to risks of abuse of this procedure and circumvention of the requirement for prior authorisation. (§ 208) 10. The law is not established to contain sufficient safeguards against the repeated use of the emergency authorisation procedure. (§ 208) 11. The court ruling on the authorisation to implement the surveillance measure has at its disposal only the material submitted to it by the State authorities requesting such authorisation in support of their application, which is likely to deprive it of the power to verify whether there is a sufficient factual basis for the implementation of covert surveillance measures. (§ 209)

	12. The court ruling on the authorisation to implement the covert surveillance measure has the option of rejecting the requesting authority's application if it considers that the application is insufficiently substantiated. However, it does not deprive the authority in question of the possibility of resubmitting its application after verifying which of the information in its possession should or could be communicated to the judge so that he may assess the necessity of implementing the surveillance measure. (§ 209) **Overall:** The ECtHR considered that the authorisation procedures existing under Polish law, as they operate in practice, are incapable of ensuring that covert surveillance measures are applied only where genuinely justified. (§ 210)
Provisions relating to the monitoring of communications covered by professional secrecy	1. Article 19 of the Police Act draws a distinction between, on the one hand, information enjoying the protection of absolute professional secrecy to which defence lawyers and priests are entitled and, on the other hand, information that enjoys a lesser degree of protection under the privilege in question, as in the case of notaries, solicitors and legal advisers (unless they are defence lawyers), tax advisers, doctors, mediators or journalists. (§ 220) 2. The substantive conditions governing the police's ability to carry out covert surveillance of communications between lawyers and their clients are the same as those applicable to the covert surveillance of members of the general public. (§ 221) 3. The competent police officers are required to destroy information covered by absolute professional secrecy. (§ 221) 4. The legislation in question does not prohibit covert surveillance of defence lawyers. (§ 221)

	5. According to Article 19 § 15 of the Police Act, the competent police officer primarily decides what should be done with information gathered in the course of covert surveillance measures, assessing, inter alia, whether the information is covered by legal professional privilege and whether it should therefore be destroyed without delay, or forwarded to the competent court for a ruling in cases where the information in question enjoys a lesser degree of protection under professional secrecy. (§ 223) ➡ ECtHR held that the decision as to the fate of information covered by legal professional privilege should be entrusted to a body external to and independent of the State authorities concerned, preferably an independent judge. (§ 223) 6. Protected information which enjoys a lesser degree of protection under professional secrecy is forwarded to the court which decides how to proceed with it. Article 19 § 15 of the Police Act requires the court to admit such evidence if "this is necessary from the perspective of the judicial system" and if there is no other means of establishing the facts. The terms "necessary from the perspective of the judicial system" are so vague as to allow for an interpretation of professional secrecy that would render it meaningless. (§ 224) **Overall:** the Court considers that the rules relating to the protection of professional secrecy in covert surveillance operations do not satisfy the criterion of foreseeability of the law. (§ 225)
Monitoring the implementation of covert surveillance measures	1. The ECtHR did not find that the Polish **courts** have the power to exercise sufficiently extensive oversight over the interception of communications. The judicial review of surveillance is limited to the initial stage of authorisation. (§ 231) 2. **Prosecutors** are involved to a certain extent in the process of prior review of surveillance, are informed of the results of the interception and, if they so request, of its conduct. (§ 232)

	➡ ECtHR found that a legal framework provides, at least in theory, for a certain degree of oversight of covert surveillance measures by prosecutors. (§ 232) 3. Public prosecutors are subordinate to the Chief Public Prosecutor of the National Public Prosecutor's Office, who also acts as Minister of Justice. (§ 233) ➡ ECtHR held that this fact alone is likely to compromise their ability to exercise independent oversight over the State surveillance services. (§ 233) 4. The scope of prosectors' oversight is limited: they must be informed of the results of operational oversight and may require the services carrying out such oversight to submit to them any relevant documents, however, they cannot order the destruction of material intercepted unlawfully. (§ 234) 5. The **parliamentary committee**, the **Sejm** and the **NIK** have no power of oversight regarding the application of interception measures in specific situations, and are not empowered to take remedial measures: they cannot annul an interception authorisation, nor bring an unlawful interception to an end, nor, finally, order the destruction of data collected unlawfully. (§ 235) 6. The annual report of Minister of the Interior to the Parliament on police surveillance operations cannot replace the oversight of specific surveillance operations by an independent body which is well acquainted with surveillance and interception practices and is not institutionally linked to the police, nor to the executive branch or the law enforcement or intelligence services. The same applies to the annual reports of head of the CBA or head of the KAS, since they provide only a general overview of surveillance activities. (§ 235) **Overall:** The ECtHR considered that the current mechanism does not guarantee effective and independent supervision of the State services carrying out surveillance and is not capable of providing adequate safeguards against abuse. (§ 237)

Notification of communications surveillance and available remedies	1. Article 19 § 16 of the Police Act prescribes that information gathered in the course of operational monitoring by police services conducting secret surveillance is not disclosed to the person who was the subject of it. (§ 238) 2. Polish legislation does not provide for any mechanism for notifying the person suspected of involvement in unlawful activities or any individual indirectly affected by the surveillance measure, unless criminal proceedings are brought against the person concerned and the intercepted data is used as evidence in the proceedings. (§ 240) 3. Person who believes they are being monitored could on the basis of section 2 of the Public Information Access Act, invite the head or heads of the police and intelligence services concerned to disclose to them the information allegedly collected without their knowledge in the course of secret surveillance, and, in the event of unfavourable decisions, challenge those decisions before the administrative courts. (§ 241) ➡ The ECtHR held that a challenge to the decisions of the heads of the police and intelligence services would be likely to fail in view of the settled case law of the Supreme Administrative Court, according to which information relating to operational investigative measures, the methods used, the agents involved and the data collected by means of the measures in question is subject to protection similar to that of classified data and may therefore only be disclosed to persons with specific authorisation. (§ 241) 4. The constitutional appeal would not have enabled the applicants to have the legality of any surveillance of them reviewed. (§ 242) 5. The exercise of an action for damages on the basis of 417-1 of the Civil Code would depend on the prior success of the constitutional appeal. (§243)

Denysyuk and Others v Ukraine (2025)	
Type of interception	Targeted interception (lawyer-client privilege)
Abbreviations	CPC — Criminal Procedure Code of Ukraine
Authorisation procedure	1. Under Articles 246, 263, 270 of the CPC, covert surveillance must be authorized by a judge based on "reasoned requests" from law enforcement, and the judge is required to provide specific reasons for the decision and may demand supporting evidence (§§ 94–95). 2. Domestic law requires judges to perform a substantive balancing exercise, weighing the public interest in combating serious crime against the individual's right to privacy under Article 8 (§ 95). 3. The ECtHR held that surveillance subjects should, by default, be granted access to the judicial rulings authorizing the measures against them so they can vindicate their rights, unless there are "compelling grounds" for denial (§ 97). But authorities denied access to these rulings solely because they were "classified," and did not to perform a balancing exercise to justify continued secrecy once the investigation was complete and the material destroyed (§ 98). **Overall:** While CPC contains formal requirements for judicial authorization and balancing tests, the Court found an Article 8 violation because the authorities failed to prove these safeguards were applied in practice and improperly used "classified" status to block individuals from reviewing the legal basis for their surveillance (§ 100). The Court invoked Rule 44C to infer that the surveillance was likely not the result of the "proper and detailed judicial scrutiny" required by law (§§ 99–100).

Scope of the legal professional privilege to be intercepted and the distinction between privileged and non-privileged material	1. The Bar and Advocacy Act establishes a general protection for legal professional privilege, covering all information exchanged between a lawyer and client. Article 258(5) of the CPC explicitly prohibits any interference with private communications between a lawyer and client during covert operations (§ 106). 2. There are no publicly available instruments or guidelines detailing the conditions or technical methods used to distinguish between privileged and non-privileged material during an active interception (§ 111). 3. The task of identifying and "screening" privileged material is assigned to law-enforcement officers, which the Court deemed unacceptable without oversight by an independent authority (§§ 104, 112).
The procedures for reporting to an independent supervisory authority for the review of cases where material subject to legal professional privilege has been acquired as a result of secret surveillance	1. Under Articles 246 and 263 of the CPC, judges are responsible for the initial authorization of covert measures (§ 95). But the judicial power ends at the authorization stage as judges have no competence to supervise the implementation of their own rulings, are not informed of the results of the surveillance, and cannot review whether the executive complied with the terms of the warrant (§ 112). 2. Supervision is instead entrusted to prosecutors, who are not considered "sufficiently independent" from the law-enforcement officers conducting the investigation. The system lacks a body capable of verifying in real-time that officers are not abusing their power or mishandling privileged data (§ 112).
The procedures for the secure destruction of the material	1. Article 255 of the CPC mandates the "immediate destruction" of intercepted material once it is qualified as irrelevant to the prosecution of the offense (§ 108). 2. While the principle of destruction is consistent with data protection, the actual implementation is shielded from scrutiny. Here, authorities refused to provide the applicants with copies of the prosecutor's decision to destroy the material or the official "act" of destruction (§ 109). Since the destruction records remain "classified" without explanation, there is no way for a surveillance subject to verify that their privileged or irrelevant data was actually erased (§ 109).

The conditions under which it may be retained and used in criminal proceedings and law-enforcement investigations	1. There is no established protocol for what happens when a suspect's privileged conversation is "accidentally" intercepted during telephone tapping or audio monitoring (§ 111).
The procedures for its safe storage, dissemination and subsequent destruction as soon as it is no longer required for any of the authorised purposes	1. Certain rules regarding the handling of covert measures are contained in the 2012 Instruction on Covert Measures (§ 111). But the 2012 Instruction contains no specific guidelines regarding the protection of lawyer-client communications. It fails to define how legal professional privilege materials should be stored or the precautions to be taken when communicating such material to other parties (§ 111, 113).
Notification and availability of post-factum remedies	1. Article 253 of the CPC requires authorities to notify subjects of surveillance within 12 months of its conclusion (or upon trial). The ECtHR viewed this as a "tangible step forward," but noted that notification is only effective if accompanied by access to the "factual and legal reasons" for the intrusion (§§ 120–121). 2. The remedial process under the CPC is flawed because the first step, *i.e.* filing complaints under Articles 303 or 309, cannot be triggered independently by the individual. Subjects must wait for a "preparatory hearing," which often leads to "unpredictable delays" that compromise the remedy's effectiveness (§ 126). 3. Article 315 of the CPC does not grant trial judges the specific power to review the underlying necessity of surveillance or the reasoning of the original authorizing judge. Instead, courts often limit their review strictly to whether the resulting evidence is admissible, ignoring the broader privacy complaint (§§ 127, 129).

	4. The refusal to grant access to "classified" judicial rulings renders specific legal objections, *e.g.* those under Article 309(3) of the CPC, "theoretical and illusory." Individuals cannot effectively challenge the legality of an order they are not permitted to read or analyze (§§ 119, 130). 5. CPC lacks the discretionary power previously found in the 1960 Code (*see* Article 23-2) that allowed judges to issue "separate rulings" acknowledging rights violations, further narrowing the pathways for a formal recognition of a breach (§ 123). 6. Since the initial procedural step in the criminal courts is effectively blocked or delayed, the secondary route (civil proceedings for compensation) cannot be accessed in "good time" and therefore fails to provide a robust judicial remedy (§ 131). **Overall:** Ukrainian law lacks sufficient procedural safeguards because it provides no independent, accessible mechanism for subjects to verify the necessity and proportionality of surveillance. The current reliance on narrow criminal court procedures and "classified" barriers makes the right to a post-surveillance remedy effectively impossible to exercise (§§ 132, 134).

Лабораторія
цифрової
безпеки

ZMINA
ЦЕНТР ПРАВ ЛЮДИНИ

Фінансується
Європейським Союзом

2026