Право на приватність

Авторка: Анна Людва, юристка Лабораторії цифрової безпеки
https://eurointegration.ccl.org.ua/expert/anna-lyudva/

Текст станом на листопад 2025 року

Це дослідження підготовлене у межах проєкту «Правосуддя для жертв війни та покращення дотримання основоположних прав в Україні», що реалізується за підтримки Європейського Союзу. Усі думки, погляди та пропозиції, викладені в цьому дослідженні, належать виключно автору(-ці) та відображають думки, погляди та пропозиції автора(-ки) та ГО «Центр громадянських свобод». Це дослідження жодним чином не відображає позиції чи політики Європейського Союзу.

center for civil liberties
центр громадянських свобод

Funded by the European Union

Автор і видавець: Громадська організація «Центр громадянських свобод»
Мови видання: українська
Посилання на сайт: https://ccl.org.ua
E-mail: office@ccl.org.ua

Рекомендоване цитування: Анна Людва. Право на приватність. *Центр громадянських свобод*. 2026. 23 с. URL: https://eurointegration.ccl.org.ua/

ЗМІСТ

Право на приватність

Потреба у модернізації українського законодавства виникала завжди з огляду на виклики цифрової ери та розвиток нових технологій, проте наразі така необхідність набуває нових масштабів. Гармонізація зі стандартами ЄС у сфері захисту приватності стає особливо актуальною в умовах наближення України до офіційного членства. Як держава-кандидат, Україна повинна адаптувати власне законодавство до європейських вимог у всіх сферах, включаючи сферу захисту персональних даних та приватності. Для належної адаптації українського та європейського законодавства, Цифролаба підготувала аналітичний звіт[1], у якому проаналізувала ключове законодавство ЄС, закони України, відповідність українських стандартів європейським, а також надала рекомендації щодо зміни чинного законодавства.

Стандарти приватності у ЄС та Раді Європи

Право ЄС

Європейське законодавство характеризується високим рівнем стандартизації та суворими вимогами в контексті захисту конфіденційності та приватності, особливо у сфері персональних даних. Обидва конституційні договори, **Договір про функціонування Європейського Союзу** та **Договір про Європейський Союз**, наголошують на захисті користувачів під час збору та обробки їх персональних даних у своїх статтях 16 та 39 відповідно.

Основоположним документом ЄС в контексті обробки персональних даних є **Загальний регламент захисту даних** (GDPR). Регламент передбачає вичерпний перелік принципів, на яких ґрунтується правомірна обробка персональних даних: законність, добросовісність та прозорість, обмеження мети, мінімізація даних, точність персональних даних, обмеження строків зберігання, цілісність та конфіденційність.[2] Принцип підзвітності випливає з обов'язку контролера дотримуватися вищезгаданих установ та нести відповідальність у випадку їх порушення.[3] Регламент також наділяє суб'єкта даних широким рядом прав для їх захисту: право на інформацію, право на доступ до персональних даних, право на виправлення даних, право на забуття, право на заперечення та обмеження обробки даних, право на мобільність персональних даних, право на захист від автоматизованого прийняття рішення, а також відшкодування шкоди та відновлення порушених прав.[4] GDPR містить чіткий механізм реагування на порушення законодавства, вирішення спорів та накладення відповідних штрафних санкцій. Він передбачає призначення офіцерів із захисту даних, а також вимогу проведення оцінки впливу на захист даних політик і практик компаній.

---

[1] Звіт: Права людини у цифровому вимірі 2024. *Лабораторія цифрової безпеки*. 18 квітня 2025. URL: https://dslua.org/publications/zvit-prava-liudyny-u-tsyfrovomu-vymiri-2024/

[2] Стаття 5(1)

[3] Стаття 5(2)

[4] Розділ III

Крім того, документ слугує базисом для дотичного законодавства ЄС, як от **Регламенту (ЄС) 2018/1725**, який регулює обробку та передачу персональних даних установами, органами, службами й агентствами ЄС у контексті судової співпраці та **Директиви (ЄС) 2016/680** про захист фізичних осіб щодо обробки персональних даних компетентними органами з метою запобігання, розслідування, виявлення чи переслідування за кримінальні правопорушення або для виконання кримінальних покарань, а також щодо вільного переміщення таких даних. На відміну від GDPR, Директива дозволяє обробку біометричних даних в цілях правоохоронної діяльності, проте виключно на підставі закону, для захисту життєво важливих інтересів суб'єкта персональних даних або іншої фізичної особи, а також якщо така обробка стосується даних, які особа явно оприлюднила. Відповідні дії з чутливими даними здійснюються тільки якщо переслідувана мета не може бути досягнута за допомогою менш інтрузивних засобів. Водночас Директива зобов'язує правоохоронні органи здійснити анонімізацію або псевдонімізацію оброблених даних після завершення розслідування для зменшення ризику порушення приватності.

Директива (ЄС) 2002/58 регулює обробку персональних даних та захист конфіденційності у сфері електронних комунікацій, фокусуючись на захисті даних користувачів інформаційних сервісів. Директива забезпечує захист вмісту всіх електронних повідомлень та мережевого трафіку, забороняючи будь-яке прослуховування, перехоплення або зберігання комунікацій без попередньої згоди користувача, за винятком випадків, передбачених законом.[5] Аналогічно, будь-які комунікаційні дії, як-от використання файлів cookie, обробка даних для маркетингових цілей або надсилання небажаних повідомлень (спаму), можуть відбуватися лише за умови попередньої згоди. Говорячи про інформаційну безпеку, слід також виокремити **Директиву (ЄС) 2016/1148** (Директиву NIS). Документ зобов'язує операторів забезпечувати безпеку даних під час надання послуг для уникнення несанкціонованого доступу або атак. У випадку кіберінциденту, оператори повинні негайно повідомити про це відповідні органи, слідуючи правилам щодо витоку даних, встановлених GDPR. Компетентні органи повідомляють користувачів про кіберінцидент лише якщо обізнаність громадськості є необхідною для його запобігання або вирішення.[6]

Регламент (ЄС) 2023/2854 (Акт про дані) та **Регламент (ЄС) 2022/868** (Акт про управління даними) законодавчо передбачають вільний обіг даних у приватному та публічному секторах. **Акт про дані** регулює доступ та обмін всіма даними (не лише персональними), згенерованими при використанні так званих "пов'язаних продуктів" (з англ. "connected product"), а також сприяє розвитку конкурентного ринку хмарних послуг. Відповідні продукти зазвичай включають об'єкти інтелектуальної діяльності, цифрових послуг та розумних машин. За своїм обсягом Акт дозволяє користувачам, тобто компаніям та особам, які володіють, беруть у лізинг або орендують відповідний продукт, отримувати доступ до даних, згенерованих у результаті його використання. Закон

[5] Стаття 5(1)
[6] Стаття 14(6)

встановлює вимоги до обміну даними у приватному секторі у форматах: “бізнес-споживач”, “бізнес-бізнес”, “бізнес-уряд”.

- У випадку відносин “бізнес-споживач” та “бізнес-бізнес”, продукти та послуги мають бути розроблені та виготовлені таким чином, аби доступ до їх даних здійснювався легко та безперешкодно: власники (розпорядники) даних (тобто особи, які розпоряджаються даними відповідного пов’язаного продукту) зобов’язані надати доступ користувачу в безпечному, безоплатному, комплексному, структурованому, широко використовуваному та машиночитабельному форматі.[7] Своєю чергою, користувачі мають право своєчасно отримувати доступ до даних та ділитися цими даними з третіми сторонами за власним вибором, за винятком брамників (з англ. “gatekeepers”) (встановлених Актом про цифрові ринки), тобто онлайн-платформ, які стали основним каналом для своїх бізнес-користувачів в охопленні споживачів.
- У контексті відносин “бізнес-уряд”, власники даних зобов’язані передати відповідні дані на вимогу публічних інституцій за наявності виняткової потреби, яка включає надзвичайну ситуацію, публічний інтерес передбачений законом (як от розробка офіційної статистики), а також вичерпання альтернативних способів отримання даних.[8]

Своєю чергою, **Акт про управління** даними регулює добровільний обмін даними з публічними інституціями, вимагаючи від Держав-членів ефективного законодавчого та технічного оснащення для належної передачі даних (наприклад, анонімізація даних, наявність спеціальних контрактів для передачі конфіденційних даних (лише за згодою суб’єкта даних)).[9] Крім того, Акт заохочує Держав-членів сприяти “альтруїзму даних”, тобто створенню умов, за яких особи можуть добровільно ділитися своїми даними на благо суспільства.[10] Оскільки надалі відповідні дані будуть оброблятися перевіреними організаціями, для підвищення прозорості Акт вимагає від Держав-членів створення та оновлення публічного національного реєстру таких організацій. Говорячи про вільний обіг даних, слід також згадати **Директиву (ЄС) 2019/1024**, що встановлює правила для вторинного використання загальнодоступної інформації, якою володіє державний сектор. Хоча Директива здебільшого регулює обмін відкритих даних, вона побічно торкається і персональних даних, вимагаючи їх обов’язкової анонімізації при передачі для захисту конфіденційності.[11] На відміну від Директиви, Акт про управління даними передбачає більш суворі правила та гарантії захисту даних, оскільки останній охоплює не лише відкриті дані, а й персональні, захищені та конфіденційні дані.

Продовжуючи тему обміну даних, варто згадати й договірні положення, встановлені GDPR, які слугують гарантіями захисту даних та можуть використовуватися як підстава для передачі даних з ЄС до третіх країн. У цьому випадку Європейська комісія

[7] Стаття 3(1)
[8] Стаття 15(1)
[9] Стаття 5
[10] Стаття 16
[11] Стаття 6

затвердила **Рішення (ЄС) 2021/915** про стандартні договірні положення для контролерів і обробників на території ЄС/ЄЕЗ та **Рішення (ЄС) 2021/914** про стандартні договірні положення для контролерів і обробників для передачі даних третім країнам. Посилаючись на вимоги GDPR, останні передбачають гарантії захисту даних для збереження їх цілісності та безпеки навіть поза межами території ЄЕЗ, які включають, зокрема, обмеження мети, прозорість, точність та мінімізацію даних, обмеження зберігання, безпеку обробки даних та механізм дій з чутливими даними.

Новоприйняті акти ЄС також містять положення щодо захисту персональних даних. Так, **Регламент (ЄС) 2022/2065** (Акт про цифрові послуги), який слугує ключовим документом у сфері регулювання платформ та їх діяльності з модерації контенту, встановлює більш жорсткі правила захисту персональних даних. Наприклад, він забороняє поширення реклами, яка здійснює профайлинг, що використовує чутливі дані.[12] **Регламент (ЄС) 2022/1925** (Акт про цифрові ринки) регулює діяльність брамників, про яких згадувалось вище, встановлюючи набір правил щодо ключових послуг платформ (як от рекламні послуги, пошукові системи), які є вразливими до неправомірних бізнес-практик. Так, платформи зобов'язані уможливити простий доступ та адаптацію інтерфейсу під потреби користувача, зокрема для зміни параметрів щодо надання або відкликання згоди у будь-який момент. У контексті захисту даних платформам забороняється обробляти персональні дані для рекламних цілей, отримані в результаті роботи сервісів третіх сторін в межах платформ, поєднувати персональні дані із різних сервісів брамника, перехресно використовувати персональні дані із відповідного сервісу брамника в інших сервісах, і навпаки, а також підключати користувачів без їх згоди до інших сервісів брамника для збору персональних даних.[13]

Своєю чергою, **Європейський акт свободи медіа** передбачає правила щодо захисту журналістів та їх джерел, встановлюючи заборону на будь-яке стеження за їх кореспонденцією (за винятком випадків, коли наявні правові підстави).[14] Крім того, нещодавно прийнятий **Регламент (ЄС) 2024/1689** (Акт про штучний інтелект) передбачає механізм використання засобів, керованих штучним інтелектом (ШІ) із врахуванням вимог щодо захисту персональних даних. Зокрема, Акт класифікує різні системи ШІ залежно від ризику для прав і свобод осіб: заборонені, високоризикові, системи з обмеженим рівнем ризику та низькоризикові системи. Акт забороняє системи ШІ, які здійснюють скрепінг зображень обличь з Інтернету чи камер стеження, ідентифікують емоції на робочих місцях чи в навчальних закладах, та класифікують людей на основі їх біометричних даних.[15] Водночас Акт дозволяє обробку особливих категорій даних провайдерам високоризикових системам ШІ виключно тою мірою, в якій це суворо необхідно для виявлення та виправлення упередженості, враховуючи відповідні гарантії для суб'єктів даних. Для здійснення такої обробки Акт вимагає наявність шести

[12] Статті 26, 28
[13] Стаття 5(2)
[14] Стаття 4(3), 4(5)
[15] Стаття 5(1)(e,f,g)

обов'язкових умов, серед яких, зокрема, неможливість виявлення та виправлення упередженості внаслідок обробки інших даних (включаючи синтетичні та анонімні дані), поширення на особливі категорії даних заходів безпеки та конфіденційності (як от псевдонімізація даних) та неможливість їх повторного використання, заборона передачі або надання доступу до відповідних чутливих даних третім особам тощо.[16]

У контексті регулювання варто також згадати керівництва Європейської ради із захисту даних – документи, розроблені для уточнення та узгодженого розуміння положень законодавства ЄС у сфері захисту даних. Наприклад, **Гайдлайни 05/2020** аналізують концепт "згоди", затверджений Загальним регламентом захисту даних, уточнюючи вимоги щодо механізму підтвердження та отримання згоди від суб'єкта даних. **Гайдлайни 01/2023** пояснюють застосування статті 37 Директиви (ЄС) 2016/680 стосовно передачі персональних даних компетентними органами Держав-членів ЄС третім урядам або міжнародним організаціям, компетентним у сфері правоохоронної діяльності. Гайдлайни також зазначають про забезпечення додаткових гарантій для належної та безпечної передачі даних третім урядам, які можуть включати: обмеження доступу до переданих даних, обмеження обробки даних до специфічної мети, визначення спеціальних умов для обробки переданих даних та встановлення механізму нагляду над передачею.[17]

При зверненні до механізмів стеження варто враховувати вимоги **Гайдлайнів 05/2022 щодо використання технологій розпізнавання обличчя у сфері правоохоронної діяльності**. Документ передбачає механізм дій перед, під час та після застосування інтрузивних технологій задля уникнення перевищення повноважень з боку правоохоронних органів та забезпечення приватності суб'єктів даних. Зокрема, перед зверненням до технологій розпізнавання обличчя від уповноважених органів вимагається окреслення суб'єктів (об'єктів), над якими буде здійснюватися стеження, перелік конкретних цілей, для яких використовуються технології, час та спосіб збирання відповідних даних, включаючи інформацію про кількість та якість отриманих біометричних даних. Після завершення використання технологій важливою є повторна перевірка отриманих результатів (яка виключає можливість автоматизованого прийняття рішення), а також встановленні механізму дій у випадку витоку даних. Правила щодо захисту суб'єктів даних при здійсненні над ними стеження містяться й у **Гайдлайнах 03/2019**, яка стосується обробки персональних даних через відеопристрої. Зокрема, для зменшення ризиків щодо приватності при обробці біометричних даних, отриманих під час відеостеження, документ пропонує контролерам даних вживати таких заходів: зберігати дані у централізованій базі даних у зашифрованому вигляді, зберігати біометричні шаблони та необроблені дані в окремих базах даних, розробити технічні методи для виявлення шахрайства, видаляти необроблені дані (як-от зображення обличчя, мовні сигнали, хода тощо) та забезпечувати ефективність такого видалення.

[16] Стаття 10(5)
[17] ст. 29

Судова практика (Суд справедливості ЄС та ЄСПЛ)

У правозастосовному контексті слід також згадати практику Європейського суду з прав людини (надалі – ЄСПЛ або Суд), який має великий вплив як на законотворчість Держав-членів та політику в межах ЄС загалом. У своїй практиці ЄСПЛ проаналізував безліч справ, які особливо стосуються сфери приватності. У цьому випадку слід виокремити ключові справи, які мали вплив на подальше регулювання правової сфери. Крім того, варто взяти до уваги й практику Суду справедливості ЄС – інституції, яка забезпечує узгоджене застосування права ЄС Державами-членами, вирішує спори між інституціями ЄС та національними урядами, а також має повноваження щодо анулювання актів ЄС та накладення санкцій на інституції у випадку порушень. У цьому випадку будуть аналізуватися справи здебільшого щодо інтерпретації права ЄС для уточнень правил та стандартів.

Стеження

Говорячи про використання засобів масового стеження, до якого вдається й Україна, ЄСПЛ загалом дотримується одностайної позиції, не забороняючи таку практику за умови наявності належних гарантій для суб'єктів даних. У своєму пілотному рішенні *Big Brother Watch and Others v the United Kingdom*, яка стосується перехоплення контенту та метаданих у Великобританії та їх передачі іноземним спецслужбам, Суд визнав, що будь-які заходи стеження повинні бути належним чином обґрунтовані та впроваджені лише компетентним органом, підлягати незалежному нагляду, а відповідна особа повинна бути повідомлена про застосування технологій. Водночас у справі *Centrum For Rattvisa v Sweden* з аналогічними фактами, ЄСПЛ визначив, що передача даних іноземним силам безпеки відповідає статті 8 Конвенції, якщо іноземний одержувач пропонує прийнятний мінімальний рівень гарантій. Серед спірних висновків ЄСПЛ в обох справах – відсутність потреби у повідомленні про стеження суб'єкта даних, що непрямо передбачено у GDPR.

У справі *Roman Zakharov v Russia* правоохоронні органи здійснювали прослуховування телефонних розмов заявника для оперативно-розшукової діяльності без правових підстав. Рішення слугує одним із ключових у практиці Суду, оскільки саме у ньому ЄСПЛ розробив набір критеріїв, за яких втручання у приватність буде виправданим та пропорційним. Серед них: доступність національного закону, обсяг таємного стеження, тривалість таких заходів, процедури, яких слід дотримуватися щодо збереження, консультацій, вивчення, використання, передачі та знищення перехоплених даних, дозвіл на перехоплення, моніторинг здійснених заходів, повідомлення про перехоплення та доступність способів правового захисту. Суд також наголосив, що національний закон, який наділяє уповноважені органи функціями щодо використання засобів стеження, повинен чітко зазначати обсяг їх дискреції та підстави для здійснення таких функцій. Аналогічного висновку ЄСПЛ досягнув і у справі *Ekimdzhiev and Others v Bulgaria*, яка стосується таємного стеження за електронними комунікаціями. Окрім вищезгаданих критеріїв, Суд також підкреслив, що національний закон повинен

містити чіткий перелік підстав для застосування таємного стеження та осіб, які можуть піддаватися такому стеженню, а також належний механізм нагляду у контексті звернення до інтрузивних засобів. Такої ж думки Суд дотримався й у справі *Klass v Germany*, де було вирішено, що позбавлене нагляду, неконтрольоване і нецільове перехоплення комунікацій порушує права людини. Примітно, що нагляд, якого вимагає Суд, повинен бути інституційно незалежним і неупередженим для виключення будь-якого виду зловживань. Це було підкреслено у справі *Szabo and Vissy v Hungary*, де нагляд від "політично заангажованого члена виконавчої влади" було визнано недостатнім для забезпечення належного захисту приватності.

Для забезпечення вимог приватності ЄСПЛ також неодноразово наголошував на наявності законодавчих гарантій для суб'єктів, над якими здійснюється таємне стеження. Так, у справі *Peck v the United Kingdom*, у якій місцеві медіа оприлюднили спробу самогубства на вулиці місті без відома особи, Суд визнав порушення статті 8 Конвенції з огляду на відсутність ефективних засобів правового захисту у випадку неправомірного розкриття інформації. У справі *Bărbulescu v Romania* працедавець здійснював моніторинг приватних листувань працівника, звільнивши його через персональне використання Інтернету на робочому місці всупереч внутрішнім правилам. ЄСПЛ визнав порушення, наголосивши, що працівник повинен бути належним чином попереджеником як про можливість моніторингу його кореспонденції, так і про можливість доступу до його персональних даних без його відома.

У справі *Perry v the United Kingdom*, що стосувалася прихованої відеозйомки затриманої особи для цілей ідентифікації, Суд визнав порушення статті 8 Конвенції, оскільки такі заходи застосовувалися без попереднього попередження особи, без його згоди на зйомку та подальше використання даних, а також без пояснення прав, якими наділений суб'єкт даних у такому випадку. Говорячи про права осіб, залучених у розслідування, слід згадати справу *Gaughran v the United Kingdom*, у якій поліція безстроково зберігала фотографію обвинуваченої особи та її біометричні дані (профіль ДНК та відбитки пальців). У цьому випадку ЄСПЛ підкреслив потребу у чітких періодах зберігання біометричних даних як чутливих даних, а також гарантій для обвинуваченого (наприклад, видалення даних якщо їх обробка більше не є необхідною). У контексті правоохоронної діяльності у рішенні *Weber and Saravia v Germany* ЄСПЛ визнав, що тяжкі та особливо тяжкі злочини можуть бути підставою для заходів загального стеження, проте лише за наявності обґрунтованої підозри. При цьому Суд визнав втручання органів виправданим, оскільки передача та використання персональних даних відповідали принципу обмеження використання даних, знищення персональних даних слугували гарантіями проти зловживань, а відповідних осіб було якнайшвидше повідомлено про обмеження таємниці їх телекомунікацій.

Справи щодо захисту кореспонденції обвинувачених були проаналізовано і в українському контексті. Суд визнав порушення в справах *Trosin v Ukraine* і *Volokhy v Ukraine*, які стосувалися таємного моніторингу повідомлень ув'язнених, оскільки

українська правова система не містить ні законодавчо визначеного обсягу та умов для стеження, ані належних гарантій проти зловживання заходами стеження.

Своєю чергою, Суд ЄС загалом віддзеркалює позицію ЄСПЛ, дозволяючи уповноваженим органам вдаватися до систем стеження, особливо за наявності легітимної мети та попередніх законодавчих гарантій. Така практика відображається у двох ключових справах Суду: *Privacy International* (щодо збору масових даних зв'язку службами безпеки та розвідки від операторів мобільних мереж) та *La Quadrature du Net* (щодо масового та автоматичного збору та обробки даних з метою виявлення терористичних атак). В обох справах Суд ЄС визначив, що право ЄС загалом забороняє невибіркове (з англ. "indiscriminate") збереження або передачу даних про трафік та локацію навіть за умови переслідування цілі національної безпеки. При цьому у справі *La Quadrature du Net*, Суд фактично дозволив використання різних систем стеження, заключивши, що невибіркове збереження даних буде вважатися законним за умови доведення Державою-членом наявності легітимних та серйозних загроз національній безпеці. Водночас, у своєму нещодавньому рішенні *HADOPI*, яке стосується питання законності масової системи стеження від урядового агентства Hadopi, Суд ЄС дещо змінив свій погляд на стеження. Суд контроверсійно визначив, що за замовчуванням доступ до IP-адрес більше не вважається серйозним втручанням у фундаментальні права, фактично дозволивши можливість масового стеження в Інтернеті.

Захист журналістів та журналістських джерел

Право на захист кореспонденції включає і недоторканність професійних комунікацій, включаючи журналістські джерела. Хоча відповідні справи ЄСПЛ розглядає здебільшого під призмою статті 10 Конвенції, право на свободу вираження поглядів у контексті кореспонденції захищається і статтею 8 Конвенції. У справі *Sedletska v Ukraine*, під час кримінального розслідування окружний суд уповноважив слідчого на доступ до телефонних даних журналістки та редакторки програми, яка висвітлювала корупцію серед політиків. ЄСПЛ визнав, що таке втручання у права заявниці не було виправданим, оскільки відкритий доступ до її даних міг призвести до розкриття її журналістських джерел. Крім того, у справі *Ukraine v Russia (re Crimea)*, ЄСПЛ визнав численні порушення проти журналістів, здійснені на окупованій території Криму з боку держави-агресора, які включали, зокрема, принизливе ставлення та незаконне ув'язнення журналістів, придушення українських медіа, анулювання ліцензій на мовлення, видачу "попереджень" українським журналістам, яких вважали "екстремістами". Захист журналістів включає також і недопущення здійснення стеження над медіа з метою подальшої передачі інформації, що може призвести до розкриття їх джерел (*Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands*).

Право на зображення

ЄСПЛ часто аналізує справи щодо приватності крізь призму свободи вираження поглядів, оскільки обидва права часто можуть суперечити одне одному. У цьому випадку правом, яке випливає із концепту приватності, є право на зображення, тобто на

поширення фотографій особи лише за її попередньою згодою. У ключовій справі *Von Hannover v. Germany (no. 2)* щодо публікації фотографій відомої пари без їх відома, ЄСПЛ виокремив основні критерії, які варто брати до уваги для оцінки правомірності втручання у приватність. Такі критерії включають: внесок у дискусію, що становить суспільний інтерес; ступінь знаменитості відповідної особи; тематика новин; попередня поведінка відповідної особи; зміст, форма та наслідки публікації; та, у відповідних випадках, обставини, за яких були зроблені фотографії.[18] Крім того, право на зображення супроводжується правом особи контролювати використання фотографії, що включає і відмову на її публікацію. Таке право поширюється і на випадки, коли відповідна інформація вже знаходиться у публічному просторі. У справі *Hájovský v. Slovakia,* де оскаржуване зображення заявниці було висвітлено у телевізійному репортажу, а потім опубліковане у статті, ЄСПЛ наголосив, що подальше поширення такої "публічної інформації" повинне балансуватися із правом заявниці на її приватність.

Приватність і доступ до публічної інформації

Практика ЄСПЛ торкнулася і справ, у яких національні органи відмовлялися надавати доступ до публічної інформації, аргументуючи свою відмову потенційним втручанням у приватність. У випадку, коли ЄСПЛ повинен збалансувати право на приватність та свободу вираження поглядів, Суд наголошує, що, незалежно від того, за якою статтею скаржаться заявники, пріоритезація обох прав повинна бути однаковою. У справі *Centre for Democracy and the Rule of Law v Ukraine*, де Центральна виборча комісія відмовилася надавати громадській організації копії CV кандидатів у парламентські вибори, ЄСПЛ виокремив такі основні критерії для оцінки наявності втручання: природа пошукової інформації, особлива роль шукача інформації в «отриманні та передачі» її громадськості, готовність та доступність пошукової інформації. Крім того, у справі *Leshchenko v. Ukraine*, де журналісту відмовили у наданні доступу до інформації для здійснення журналістського розслідування, ЄСПЛ вказав, що національні органи потенційно можуть обмежити обсяг розкриття пошукової інформації, проте за наявності чітко сформульованих законодавчих винятків щодо приватності та конфіденційності такої інформації.

Право на забуття

У контексті права на забуття ЄСПЛ аналізував здебільшого справи, що стосуються заходів, яких можуть вжити пошукові оператори або видавці новин. Йдеться, наприклад, про видалення, зміну або анонімізацію архівованої статті або обмеження доступності інформації у мережі (наприклад, деіндексація). У випадку визнання порушення ЄСПЛ не дотримується одностайної позиції. Так, у справі *M.L. and W.W. v. Germany*, дві особи, які були засуджені за вбивство та звільнені через 14 років, вимагали у ЄСПЛ вилучення з веб-архіву газети їх фотографій, а також імен і прізвищ. ЄСПЛ не задовольнив цю скаргу, посилаючись на наявність публічного інтересу в існуванні відповідної інформації.

[18] Von Hannover v. Germany (no. 2) [GC], §§ 109- 113

Контроверсійно ЄСПЛ не проаналізував таких релевантних фактів справи: вимог заявників щодо анонімізації інформації, відсутності заявників бажання бути в межах уваги медіа, а також відомість заявників публіці завдяки опублікованій статті. Аналогічно, Суд визнав правомірною вимогу судів щодо анонімізації статті в онлайн-архіві у справі *Hurbain v Belgium*. При цьому ЄСПЛ наголосив, що принцип збереження цілісності архівів преси, зміна та їх видалення повинні бути обмежені лише у випадку суворої необхідності для запобігання "охолоджуючого ефекту" на виконання пресою свого завдання щодо поширення інформації та ведення архіву.

Говорячи про практику ЄС, Суд справедливості ЄС вперше деталізував концепт права на забуття у своєму пілотному рішенні *Google Spain*, де заявник вимагав від Google видалення пошукових посилань на опубліковані повідомлення щодо його банкрутства. У цьому випадку Суд ЄС наголосив на праві особи вимагати видалення своїх даних, якщо такі дані є "*неадекватними, нерелевантними або більше не актуальними, або надмірними по відношенню до цілей, для яких вони були оброблені, і з огляду на час, що минув*".[19] Крім того, Суд підкреслив обов'язок Google як контролера даних щодо видалення пошукових посилань на інформацію, опубліковану третіми особами, у випадку введенні імені відповідної особи у пошуковий запит. Пізніше у рішенні *Google Inc v Commission nationale de l'informatique et des libertes (CNIL)* Суд уточнив обов'язки контролера у контексті територіального обсягу, вказавши, що право на забуття, передбачене правом ЄС, не вимагає від пошукових систем видалення (з англ. "de-listing") результатів пошуку в глобальному масштабі, а лише в межах території ЄС.

Приватність у розрізі протидії дискримінації

Концепт "приватності" також тісно взаємопов'язаний із захистом "сімейного життя" та "житла", особливо якщо справа стосується атак або незаконного руйнування будинків. Якщо відповідні атаки мотивовані упередженим ставленням, ЄСПЛ розглядає такі справи, аналізуючи статтю 8 у поєднанні зі статтею 14 Конвенції щодо заборони дискримінації. Наприклад, у пілотному рішенні *Burlya and Others v Ukraine*, яка стосувалася масового нападу на будинки ромів, мотивованого антиромськими настроями, Суд визнав порушення з огляду на нездатність поліції належним чином захистити мешканців від заздалегідь спланованої атаки та припинити втручання у їх приватне життя. ЄСПЛ зобов'язав Україну сплатити заявникам компенсацію ще у 2018 році, проте рішення досі залишається невиконаним.

Приватність як спосіб протидії домашньому насильству

ЄСПЛ також розглядав справи, пов'язані з бездіяльністю влади щодо протидії домашньому насильству, що також входить до обсягу концепції приватності. У справі *Levchuk v Ukraine*, національні суди відмовили заявниці у задоволені її вимоги щодо виселення її колишнього чоловіка, який вчиняв щодо неї психологічне та сексуальне насильство. Визнавши порушення статті 8, ЄСПЛ вказав, що Україна не містить належної

[19] Google Spain case, para 94

правової системи захисту щодо протидії домашньому насильству та запропонував такі рекомендації: імплементувати виселення кривдника із житла як один із засобів правового захисту прав постраждалої особи, забезпечити ефективну роботу правоохоронних органів і соціальних служб щодо належного реагування на випадки домашнього насильства, а також забезпечити належну роботу судів щодо розгляду відповідних справ.

Приватність онлайн

Право на приватність та свободу вираження поглядів в Інтернеті включають і невід'ємне право на анонімність, оскільки позбавлення такого права в онлайн-просторі неодмінно призводить до охолоджуючого ефекту на свободу вираження та загрозу приватності. Втім, практика ЄСПЛ щодо права на анонімність залишається неоднозначною та подекуди контроверсійною. У своєму пілотному рішенні *Delfi AS v Estonia*, де компанія понесла відповідальність за образливі анонімні коментарі, опубліковані на її новинному порталі, Суд не знайшов порушення прав заявника. Однією з причин відповідальності заявника стала анонімність коментаторів, за якої було неможливо їх ідентифікувати. Аналогічно контроверсійним є і рішення *Breyer v Germany*, у якому Суд визнав правомірним законодавчий обов'язок постачальників послуг щодо збереження персональних даних користувачів передплачених SIM-карток та надання таких даних органам влади за їх вимогою. У цій справі Суд фактично проігнорував неможливість анонімного спілкування заявниками через мобільні телефони з огляду на подальший збір їх даних постачальниками послуг. Пізніше ЄСПЛ дещо змінив свій підхід до анонімності: у справі *Standard Verlagsgesellschaft mbH v. Austria (no. 3)* ЄСПЛ визначив, що національні суди порушили свободу вираження поглядів заявника, змусивши його розкрити ідентичності осіб, які залишили образливі коментарі на його веб-сайті у рамках політичних дебатів.

Приватність у кримінальній юстиції

Відповідно до ЄСПЛ, приватність гарантує "приватне соціальне життя", що може включати професійну діяльність. При цьому ЄСПЛ наголосив, що особи не можуть посилатися на статтю 8 для того, щоб скаржитися на особисті, соціальні, психологічні та економічні обставини страждання, які є передбачуваним наслідком їх власних дій. Це було підтверджено у справі *Denisov v Ukraine*, яка стосувалася усунення судді (заявника) з посади голови Київського апеляційного адміністративного суду. ЄСПЛ визнав скаргу неприйнятною у контексті приватності, оскільки причини звільнення заявника не були пов'язані з його приватним життям, а наслідки його страждань після звільнення не були достатньо суворими для того, щоб викликати застосування цього положення Конвенції. Водночас Суд визнав порушення права заявника на справедливий судовий розгляд, зауваживши, що орган, залучений у звільнення судді, не був достатньо упередженим та незалежним (більшість членів органу були залежними від державного апарату).

Оприлюднення персональних даних

У випадку розкриття персональних даних ЄСПЛ часто аналізує наявність попередньої згоди суб'єкта даних на передачу, розкриття або публікацію його даних, проте наголошує, що критерій згоди в окремих випадках часто не є вирішальним та не обов'язково призводить до порушення права на приватність. У справі *Mosley v the United Kingdom*, видавець опублікував в газеті таємно зроблені фотографії, які нібито розкривали сексуальні дії заявника, що містили нацистський підтекст. ЄСПЛ вирішив, що у цьому випадку вимога попередньої згоди не є обов'язковою, враховуючи що її наявність може мати як охолоджуючий ефект на подальші публікації журналістами, так і підірвати потребу "публічного інтересу" в отриманні необхідної інформації. ЄСПЛ також вказав, що газети та репортери достатньо добре розуміють концепт "приватного життя", аби мати змогу визначити, коли відповідна публікація може порушити право на повагу до приватного життя. Окрім діяльності медіа, ЄСПЛ зазначив, що відсутність згоди при оприлюдненні даних не становить порушення, якщо таке розкриття даних було обумовлено легітимними цілями, як от необхідністю розслідування кримінального правопорушення, забезпеченням публічності судового провадження або потребою захисту публічного здоров'я.

Українське законодавство

Українське законодавство у сфері захисту приватності містить недостатні гарантії для суб'єктів даних, потребуючи модернізації положень з огляду на їх застарілість та нездатність йти в ногу із цифровою ерою.

Основним законом, який регулює захист даних, є **Закон України "Про захист персональних даних"**, прийнятий у 2010 році. Закон регулює механізм обробки персональних даних, в тому числі із застосуванням автоматизованих засобів, та захист суб'єктів даних від неправомірного втручання у їх приватність. Варто підкреслити, що Закон сформульовано у загальних термінах, в яких відсутня деталізація та уточнення окремих механізмів дій з персональними даними. Такі формулювання змушують громадян вдаватися до широкого тлумачення закону без ефективної можливості реалізувати власні права або передбачити наслідки власних дій. Загалом положення Закону базуються на вимогах GDPR: вони окреслюють вичерпний перелік підстав для обробки персональних даних та наділяють суб'єктів даних рядом прав, реалізація яких необхідна для захисту від неправомірних дій. У контексті дій із чутливими даними Закон забороняє обробку біометричних даних за умови відсутності законних підстав для такої обробки. Водночас, Закон все ще не регулює специфіку захисту даних та не адресує основних концептів, закладених у GDPR. Положення закону не містять прямого посилання на основоположні принципи обробки даних, згадуючись дотично в окремих статтях. Вони не адресують механізму дій операторів у випадку вчинення неправомірних дій, як-от несанкціонованого доступу до даних, їх збору або небезпеки витоку. Не дивлячись на ряд покладених прав, у випадку потенційних порушень Закон не наділяє суб'єктів даних ефективними способами для правового захисту, що підвищує небезпеку

втручання у їх приватність з боку уповноважених органів. Нарешті, у Законі відсутній механізм збору та обробки персональних даних, отриманих під час використання засобів стеження, незважаючи на використання Україною передових цифрових інтрузивних технологій.

У контексті забезпечення виконання зобов'язань слід згадати **Закон України "Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних"**, який уповноважує Омбудсмена України здійснювати контроль за дотриманням законодавства про захист персональних даних. Основні завдання Омбудсмена включають отримання пропозицій та скарг від громадян, проведення перевірок, видачу приписів про запобігання або усунення порушень закону, надання рекомендацій про застосування положень закону та взаємодію з іншими органами, уповноваженими на захист даних.[20] Примітно, що Омбудсмен є єдиним контролюючим органом у сфері захисту даних, уповноважений здійснювати нагляд фактично за будь-якими діями з персональними даними. Очевидно, що таке функціональне навантаження великою мірою знижує загальну ефективність органу. Це додатково підтверджується тим фактом, що Омбудсмен не містить повноважень, пов'язаних із забезпеченням виконання законодавства. З огляду на лімітований обсяг функціоналу Омбудсмена, який не уповноважений навіть на накладення мінімальних санкцій, такий механізм контролю важко назвати ефективним.

Закон України "Про електронні комунікації", який регулює сферу електронних комунікацій та комунікаційних послуг, містить положення, спрямовані на захист користувачів відповідних послуг та їх персональних даних. Зокрема, Закон забезпечує конфіденційність комунікаційних послуг користувача, покладаючи на постачальників відповідальність за схоронність отриманих даних, дозволяючи доступ до такої інформації лише у правоохоронних цілях.[21] Закон також забороняє умисне розсилання небажаних повідомлень (спаму) на електронну пошту користувача без його згоди.[22]

Незважаючи на практику українських органів щодо використання засобів стеження (часто оснащених технологіями ШІ), Україна не містить єдиної правової бази щодо регулювання цієї сфери. Деякі посилання щодо використання цифрових технологій містяться у окремих законодавчих положеннях, які регулюють здебільшого дискрецію органів, уповноважених на здійснення стеження.

Загалом функції щодо здійснення стеження покладаються на органи безпеки та правоохоронні органи, які переслідують мету захисту національної безпеки та дотримання правопорядку. **Закон України "Про Національну поліцію"** дозволяє поліції використовувати *"фото – і відеотехніку, у тому числі техніку, що працює в автоматичному режимі"*, а також *"спеціалізоване програмне забезпечення для здійснення аналітичної обробки фото – та відеоінформації"*.[23] У цьому випадку на

[20] Стаття 23
[21] Статті 119, 121
[22] Стаття 120
[23] Стаття 40

правоохоронні органи не накладається жодних обмежень, окрім зобов'язання використовувати спостереження для чітко визначеної мети. В силу Кримінального процесуального кодексу, слідчий або прокурор мають доступ до інформаційно-комунікаційних систем досудового розслідування, які містять дані, зібрані з технічних пристроїв, в тому числі з фото- або відеокамер стеження, які функціонують у публічних місцях.[24] Крім того, кодекс уповноважує правоохоронні органи вдаватися до негласних розшукових дій (наприклад, аудіо- та відеоконтроль особи, арешт, огляд і виїмка кореспонденції), але лише у випадку підозри вчинення тяжких або особливо тяжких злочинів та якщо переслідувана мета не може бути досягнута за допомогою інших заходів. Згідно із **Законом України "Про оперативно-розшукову діяльність"**, уповноважені органи мають право здійснювати відео- та аудіоконтроль за особою, знімати інформацію з електронно-комунікаційних мереж та здійснювати спостереження за особою,[25] але виключно для досягнення легітимної цілі, вичерпний перелік яких передбачено у законі. Аналогічно, за **Законом України "Про контррозвідувальну діяльність"**, органи та підрозділи СБУ уповноважені здійснювати спостереження за особою, але лише в цілях національної безпеки.[26]

Вищезгадані закони мають проблеми надмірного обсягу дискреції, відсутності гарантій для суб'єктів даних та відсутності контрольного механізму. Закони, хоча і деталізують функції правоохоронних органів, не містять жодних індикаторів щодо обмеження їх дискреції в певних випадках та чітких підстав, за яких вони можуть вдаватися до засобів стеження. Говорячи про мінімальні гарантії, суб'єктів, які піддаються стеженню, не повідомляють про його здійснення, а після їх завершення не наділяють можливістю оскаржити такі дії. Це зумовлено також і відсутністю судового перегляду заходів на їх правомірність, не дивлячись на те, що першочергова авторизація надається саме судом. Нарешті, у законодавстві не передбачений наглядовий механізм, особливо у контексті інституційної незалежності. З огляду на те що аналогічний орган на практиці здійснює як стеження, так і подальше звітування щодо здійснених заходів, постає питання щодо упередженого моніторингу та розгляду.

Для модернізації законодавства у Верховній Раді було зареєстровано чимало законопроєктів, спрямованих на наближення законів до європейських стандартів та практики. Для посилення захисту суб'єктів даних у 2022 році до парламенту внесли, **Проєкт Закону №8153 про захист персональних даних**, який майже повністю базується на GDPR та фактично віддзеркалює правила та вимоги документа. У 2023 році було надано висновок головного комітету про розгляд Проєкту, проте з того часу суттєвих кроків зроблено не було.

Для адаптації європейського законодавства було зареєстровано і **Проєкт Закону №6177 про Національну комісію з питань захисту персональних даних та доступу до публічної інформації**, який запроваджує новий контролюючий орган у сфері захисту

[24] Стаття 106-1
[25] Стаття 8
[26] Стаття 7

даних. Проєкт передбачає процедуру створення, функціонування та структуру Національної комісії, а також основні повноваження та завдання. Окрім забезпечення виконання правил щодо захисту даних, Проєкт наділяє комісію функціями, відсутніми у діючого наглядового органу, тобто Омбудсмена. Зокрема, комісія уповноважена притягувати до відповідальності посадових суб'єктів контролю за порушення закону, здійснювати провадження за скаргами постраждалих осіб та накладати штрафи у випадку невиконання вимог законодавства. Проєкт знаходиться на опрацюванні з 2021 року, і з того часу суттєво не прогресував. Втім, першочерговий текст Проєкту вже містить проблемні аспекти у контексті створення нового органу, які включають бюджетні витрати на створення органу, його структуру та потенційну залежність від державного апарату.

Крім того, варто згадати Проєкти **№9250** та **№9250-1**, спрямовані на внесення змін до Закону України "Про електронні комунікації" для протидії фішингу.

Проєкт Закону №11031 про єдину систему відеомоніторингу стану публічної безпеки став однією з перших ініціатив, який прямо адресує механізм відеостеження. Його положення спрямовані на уніфікацію правил щодо використання засобів стеження шляхом розробки функціональних і технічних вимог, а також врегулювання єдиної платформи відеоспостереження в Україні. Проєкт окреслює загальні підстави для здійснення відеомоніторингу, суб'єктів, уповноважених на стеження, та об'єктів, над якими воно здійснюється. Проєкт у своїй першочерговій редакції суперечить ряду міжнародних стандартів та потребує перегляду з огляду на такі проблеми: посягання на приватність, надмірно широка дискреція державних і муніципальних органів, відсутність контролю за дотриманням законодавства, небезпека захоплення даних та технічні проблеми власне системи відеомоніторингу.

Проєкт Закону №11228-1 щодо врегулювання питань протидії розвідувально-підривній діяльності спеціальних служб іноземних держав вносить зміни до Закону України "Про контррозвідувальну діяльність". Проєкт уповноважує контррозвідувальні суб'єкти на створення інформаційних систем та баз даних для збору та зберігання інформації. Крім того, Проєкт дозволяє органам СБУ мати прямий і автоматизований доступ до систем та баз даних (включаючи конфіденційну інформацію), які адмініструються державними та місцевими органами. Контекстуально Проєкт значно розширює існуючу дискрецію органів безпеки без внесення змін до профільних законів органів, надаючи останнім необмежений доступ до персональних даних за умови відсутності легітимних підстав. Наразі Проєкт очікує на друге читання, проте навіть чинна доопрацьована редакція потребує повторного перегляду.

З огляду на тривалий воєнний стан, органи безпеки в Україні вживають заходів для захисту не лише національного, а й інформативного простору від неправомірних дій держав-агресора. Серед таких заходів – реєстрація **Проєкту Закону №11115 про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація**, який має на меті покладення обов'язків на платформи, серед яких і Телеграм. Зокрема, проєкт зобов'язує провайдерів платформ оприлюднити інформацію про власні контактні дані,

таким чином, забороняючи наявність анонімних каналів. Радикальні заходи обумовлюються загрозою національній безпеці, оскільки російські спецслужби нібито мають прямий доступ до особистої кореспонденції та навіть видалених повідомлень у месенджері. Такі заходи, хоча і переслідують легітимну мету, йдуть в розріз із реалізацією права людини на анонімність та у майбутньому безумовно створюватимуть охолоджуючий ефект на користувачів, особливо якщо йдеться про свободу вираження поглядів меншин або маргінальних груп. Попри те, що Проєкт досі перебуває на опрацюванні, відображаючи його положення, у вересні 2024 року Національний координаційний центр кібербезпеки прийняв рішення обмежити використання Телеграму в органах державної влади, військових формуваннях, на об'єктах критичної інфраструктури.

Рекомендації для зміни українського законодавства

Для належної гармонізації українського та європейського законодавства законотворцям необхідно в першу чергу внести зміни до **Закону України "Про захист персональних даних"**, оскільки він слугує базисом та орієнтиром для іншого масиву законодавства. Наразі український закон **не адресує багатьох вимог GDPR**, спрямованих на посилений захист даних, а тому в українське законодавство необхідно імплементувати такі положення:

- **Передбачити основоположні принципи обробки персональних даних.** Український закон зазначає деякі принципи у статті 6 Закону, яка регулює загальні вимоги до обробки персональних даних. Втім, їх варто деталізувати та розширити. Наприклад, посилання на принцип "обмеження мети" міститься у пунктах 1 та 5 згаданої статті, за якими вимагається законодавче формулювання мети обробки даних, що здійснюється для конкретних та законних цілей. Також Закон не містить уточнень щодо того, які цілі можуть вважатися легітимними, фактично дозволяючи їх формулювання у загальних термінах. Потреба у деталізації та чіткості формулювань мети є особливо суттєвою при зверненні до практик стеження, коли правоохоронні органи зазначають одразу декілька цілей для виправдання легітимності використаних засобів. Принцип "мінімізації даних" міститься у пункті 3 статті 6, за яким "*склад та зміст персональних даних мають бути відповідними, адекватними та ненадмірними стосовно визначеної мети їх обробки*".[27] Водночас у Законі відсутнє будь-яке посилання на принцип "обмеження зберігання", за яким персональні дані повинні зберігатися не довше, ніж це необхідно для цілей, в яких вони обробляються, за винятком випадків, встановлених законом.
- **Імплементувати "право на забуття".** В українській правовій системі відсутній концепт "права на забуття", тобто права на повне знищення контролером його персональних даних без надмірної затримки. Закон не містить механізму реалізації права на забуття, а також легітимних випадків, за яких таке право не застосовується, а

[27] Закон України "Про захист персональних даних"

обробка даних є необхідною (наприклад, для цілей архіву та підтримки електронних баз даних про кримінальні правопорушення, що мають обмежений доступ).

- **Розширити існуючий перелік прав суб'єктів даних.** У контексті прав, якими наділений суб'єкт даних, Закон все ще не містить ряду гарантій для запобігання неправомірних дій та втручання у приватність. Крім того, Закон наділяє суб'єктів даних правом "*застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних*",[28] проте не містить жодних індикаторів щодо переліку таких засобів. Наразі Закон передбачає захист персональних даних шляхом скарг до Омбудсмена та у судовому порядку (стаття 22). У цьому випадку слід розширити перелік засобів правового захисту, додавши, зокрема, механізм діалогу із незалежним регулятором. Крім того, варто деталізувати статтю 22(1)(2) у контексті судового захисту, передбачивши механізм його здійснення і гарантії для скаржника (як-от, зазначити, що особа може оскаржувати як дії наглядового органу, так і дії контролера даних).
- **Передбачити додаткові гарантії щодо обробки чутливих даних.** Говорячи про обробку біометричних даних, до якої часто вдаються правоохоронні органи з огляду на використання засобів стеження, Закон не передбачає додаткових гарантій у випадку обробки чутливих даних. Так, слід передбачити не лише функції органів при обробці та зберіганні біометричних даних, а й додаткові гарантії для суб'єкта даних, які можуть включати: обмеження строків зберігання, обов'язок знищення даних або можливість анонімізації даних після досягнення мети їх обробки. Слід також розробити механізм реагування у випадку витоку чутливих даних.
- **Регулювання профайлингу**. Закон повинен імплементувати правила GDPR щодо захисту суб'єктів даних від профайлингу – практики, яка має місце під час використання інтрузивних засобів (як-то системи розпізнавання обличчя) та ідентифікації особи за допомогою її біометричних даних. Згідно з правилами, уповноважені органи повинні чітко пояснити та обґрунтувати, у чому необхідність збору та зберігання персональних даних, та як вони допоможуть у досягненні переслідуваної мети.
- **Призначити новий контролюючий орган або розширити повноваження існуючого органу у сфері захисту даних.** Для ефективного виконання положень закону GDPR вимагає наявність належного наглядового механізму. У контексті зовнішнього контролю Регламент (ЄС) 2018/1725 уповноважує European Data Protection Supervisor здійснювати моніторинг обробки даних з боку ЄС інституцій. Український наглядовий механізм представляє обмежену та слабку систему. Наразі в українському Законі щодо захисту даних наявний лише один внутрішній наглядовий орган, яким є Омбудсмен України. Стаття 23 Закону демонструє, що функції Омбудсмена обмежені видачею рекомендацій та виїзними перевірками. Закон не наділяє контролюючий орган повноваженнями щодо самостійного вирішення спорів між суб'єктами даних та уповноваженими особами або накладення будь-якого виду санкцій. З огляду на це, необхідно встановити ефективний наглядовий орган для забезпечення виконання вимог законодавства.

[28] П.9, Стаття 8

- **Запровадження інституту офіцерів із захисту даних**. GDPR вимагає від Держав-членів призначення офіцерів із захисту даних для внутрішнього нагляду за процесами обробки персональних даних. Такий механізм має бути передбачено окремою статтею Закону з детальними вимогами до таких осіб, їх незалежності та порядку діяльності.
- **Розробити механізм реагування на правопорушення та пропорційний санкційний механізм.** Потреба у наглядовому механізмі випливає також і з факту відсутності механізму відповідальності за недотримання законодавства у сфері даних. Стаття 28 Закону сформульована у загальних термінах, не даючи можливість передбачити наслідки власних дій: "*порушення законодавства про захист персональних даних тягне за собою відповідальність, встановлену законом*". Своєю чергою, Закон не передбачає механізму реагування у випадку вчинення неправомірних дій, наприклад, несанкціонованого збору даних, недотримання термінів обробки даних або витоку персональних даних.

Узагальнюючи всі види неправомірних дій, Закон не містить ефективного санкційного механізму, що передбачає накладення пропорційних санкцій залежно від виду порушення. Відповідальність за невиконання вимог закону у сфері даних наразі прямо передбачена у Кодексі України про адміністративні правопорушення (стаття 188-39) та у Кримінальному кодексі України (стаття 182), проте лише щодо конфіденційної інформації. Таким чином, Закон України "Про захист персональних даних" варто доповнити статтями щодо накладення диверсифікованих санкцій залежно від виду та тяжкості порушення законодавства, а за умови вчинення неправомірних дій з персональними даними, які досягли рівня злочину – передбачити або деталізувати відповідні статті у Кримінальному кодексі.

Закон "Про захист персональних даних" повинен **інкорпорувати вимоги Акту про управління даними**, а саме:

- **Розробити законодавчі положення щодо обміну даних для цілей тренування ШІ-систем.** У контексті обігу даних Стаття 14 Закону регулює передачу персональних даних третім особам, яка здійснюється лише за згодою суб'єкта даних за виключенням вичерпного переліку випадків, передбачених законом, як-от: в інтересах національної безпеки, економічного добробуту, прав людини та для проведення Всеукраїнського перепису населення. Наразі Україна активно залучена до розвитку системи ШІ, а власне розробники ШІ-систем зіштовхуються з проблемою легітимного збору відкритих навчальних даних для цілей тренування машинних моделей. Оскільки в українському законодавстві не передбачено механізму обміну даних між публічними інституціями та локальними стейкхолдерами, варто розробити законодавчі положення щодо обміну даних за прикладом Європейського Акту про управління даними. Такий обмін передбачає обов'язкову згоду суб'єкта даних на передачу даних, а також наявність спеціальних договорів, що які окреслюють дії з персональними даними;
- **Запровадити концепцію "альтруїзму даних".** Закон передбачає можливість передачі відомостей про фізичну особу, проте лише за її згодою (стаття 14).

З огляду на це, у Законі варто прописати заохочувальні механізми, за яких особа зможе добровільно ділитися власними даними та умови, за яких використання таких даних було б правомірним. Ці механізми повинні обов'язково супроводжуватися гарантіями захисту отриманих даних, які включають наявність відповідних реєстрів даних та перевірених організацій, що здійснюють перевірку достовірності даних.

Для забезпечення належного захисту комунікацій користувачів, **Закон України "Про електронні комунікації" повинен адресувати вимоги Директиви (ЄС) 2002/58**, а саме:

- **Доповнити Закон основними концепціями Директиви.** Статті, які регулюють конфіденційність комунікаційних послуг, варто доповнити положеннями про запобігання можливості прослуховування та перехоплення. Крім того, для додаткового захисту суб'єктів даних, закон повинен передбачити вимогу щодо знищення або анонімізації отриманих даних, які більше не становлять потреби для надавачів комунікаційних послуг або по спливу певного строку.

Оскільки українські правоохоронні органи та органи безпеки активно використовують засоби стеження (включаючи системи, оснащені ШІ-елементами, як-от системи розпізнавання обличчя), українським законотворцям **необхідно розробити уніфікований механізм використання засобів стеження**, а саме:

- **Розробити законодавче визначення "масового стеження"**, включаючи стеження з використанням інтрузивних засобів, а також загальний механізм його використання. Наразі відповідна дефініція відсутня у будь-якому українському законі.
- **Доповнити закони України положеннями, які встановлюють легітимну мету та підстави для використання засобів стеження**. Для зниження можливостей звернення до засобів стеження у будь-яких випадках, закон повинен передбачити вичерпний перелік цілей та легітимних підстав, за яких можуть здійснюватися заходи стеження. У деяких законах, як-от Законі України "Про контррозвідувальну діяльність", такі цілі сформульовані у загальних формулюваннях (наприклад, "для цілей національної безпеки"), відкриваючи поле для широкого тлумачення. В інших випадках, як-от Законі України "Про Національну поліцію", посилання на легітимну мету відсутнє взагалі.
- **Внести відповідні зміни до профільних законів органів, уповноважених на стеження.** Для підвищення легітимності вчинених заходів, закон також повинен передбачити чітку дискрецію органів, уповноважених використовувати засоби стеження. Наразі українське законодавство не містить переліку уповноважених органів, переліку їх функцій, ані не передбачає жодних обмежень у наданих повноваженнях. У цьому випадку слід внести відповідні зміни до профільних законів про органи, уповноважені на стеження, передбачити обсяг їх дискреції, основні завдання та функції, а також потенційні "червоні лінії" як запобіжники зловживанням.
- **Розробити механізм обробки персональних даних у правоохоронних цілях.** Наразі Закон України "Про захист персональних даних" не містить належних гарантій при обробці біометричних даних, як вимагається Директивою 2016/680. У цьому

випадку обробка даних повинна відбуватися з наголосом на принципах мінімізації даних та обмеження зберігання. Якщо зберігання чутливих даних відбувається з метою запобігання або виявлення правопорушень, положення закону повинні належним чином розрізняти персональні дані окремих категорій суб'єктів даних, як-от: підозрюваних, жертв, злочинців тощо. Аналогічно, період зберігання даних повинен пропорційно залежати від тяжкості злочину, в якому підозрюється особа. Така потреба є суттєвою, оскільки наразі строк зберігання даних, отриманих із систем відеостеження, є незмінним як щодо осіб, які підозрюються у вчиненні злочинів, так і щодо інших громадян.

- **Передбачити ряд прав та гарантій для суб'єктів даних, які стають об'єктом стеження.** Наразі українське законодавство не передбачає концепту попередження, тому закон повинен містити положення про обов'язкове повідомлення особи про здійснення стеження (перед такими заходами або після них, якщо стеження необхідне для запобігання злочину). Закон також повинен зобов'язувати уповноважені органи здійснювати роз'яснення суб'єкту даних його прав (включаючи право на заперечення обробки даних або видалення його даних). Особа також повинна мати змогу реалізовувати право на оскарження здійснених заходів стеження у судовому порядку, якщо вона має підозру у їх неправомірності. Якщо стеження відбувається із використанням інтрузивних технологій (наприклад, систем розпізнавання обличчя), закон повинен містити додаткові гарантії для суб'єкта даних, серед яких обмеження періоду зберігання біометричних даних або встановлення механізм видалення даних у випадку, якщо спостереження досягло своєї мети й дані більше не є релевантними.
- **Передбачити ефективний контрольний механізм у сфері масового стеження.** Наразі українські закони не забезпечують ефективного дотримання законодавства для належного виконання покладених завдань. Деякі із законів, як-от Закон України "Про оперативно-розшукову діяльність" дозволяє вдаватися до заходів стеження лише за наявності попереднього судового дозволу, проте суди у такому випадку мають малу ефективність з огляду на відсутність судового перегляду заходів. Законодавство демонструє, що у більшості випадків орган, що уповноважений на здійснення стеження, надалі здійснює перегляд таких заходів без попереднього звітування органам, які надали авторизацію на стеження. Щобільше, такий орган не наділений функціями щодо перегляду рішення у випадку підозри неправомірності заходів стеження – на це просто відсутня встановлена законом процедура. Таким чином, необхідно створити інституційно незалежний орган, який здійснюватиме моніторинг заходів стеження, починаючи від винесення судового дозволу і закінчуючи наглядом за обробкою та зберіганням отриманих даних.
- **Встановити санкційний механізм у сфері масового стеження.** У контексті ефективного дотримання вимог законодавства Кримінальний Кодекс України повинен передбачити пропорційні санкції за несанкціоноване використання заходів масового стеження (враховуючи застосування ШІ-систем). Додаткових змін також потребує стаття

188-39 КУпАП, що стосується відповідальності за порушення у сфері захисту персональних даних.