

**ПРАВО НА ПРИВАТНІСТЬ У ЦИФРОВУ ДОБУ
КРИЗЬ ПРИЗМУ СУДОВОЇ ПРАКТИКИ УКРАЇНИ
ТА ЄВРОПЕЙСЬКОГО СОЮЗУ**

Гарашенко В. В.

*аспірант відділу теорії держави і права,
Інститут держави і права імені В. М. Корецького
м. Київ, Україна*

<https://orcid.org/0009-0004-8389-0869>

Питання захисту приватності у цифрову добу виходить за межі суто прикладного правозастосування та стає центральною темою теоретико-правових досліджень. Право на приватність трансформується з класичного елементу особистих немайнових прав у самостійний міждисциплінарний феномен, що поєднує в собі правові, етичні, технологічні та соціальні аспекти.

У теорії права спостерігається переосмислення традиційних категорій, зокрема публічного й приватного, меж державного втручання, дискреційності у правозастосуванні та принципу правової визначеності. Право на приватність у цифровому контексті викликає потребу в оновленні правових доктрин і формуванні нових понять, таких як «цифрова автономія», «алгоритмічна дискримінація» чи «інформаційний суверенітет особи».

Таким чином, тема приватності є надзвичайно важливою для теорії права, адже дозволяє не лише адаптувати класичні концепти до умов цифрового суспільства, а й розробляти нові правові механізми, які відповідатимуть викликам майбутнього.

У цифровому суспільстві саме інформація про особу, її персональні дані, стає ключовим об'єктом втручання у приватну сферу. Тому захист приватності дедалі частіше реалізується через механізми правового регулювання обробки персональних даних. Іншими словами, право на приватність виступає ширшим концептом, тоді як захист персональних даних є його конкретним інструментом і юридичною формою реалізації. Саме тому аналіз приватності в цифрову епоху органічно переходить до вивчення системи міжнародних і національних норм щодо захисту персональних даних.

Захист персональних даних є одним із ключових напрямів розвитку сучасного права, як на міжнародному рівні, так і на рівні національного законодавства.

На міжнародному рівні правове регулювання захисту персональних даних ґрунтується на багаторівневій системі джерел, яка включає універсальні та регіональні міжнародні договори, стандарти Ради Європи та нормативні акти Європейського Союзу. Цифровізація суспільства та зростання ролі штучного інтелекту в ухваленні рішень актуалізували потребу в оновленні підходів до забезпечення фундаментального права на приватність, гарантованого статтею 8 Конвенції про захист прав людини і основоположних свобод.

Першим універсальним міжнародним документом у сфері захисту персональних даних стала Конвенція Ради Європи № 108 (1981 р.) [1], яка заклала принципи законності, пропорційності, безпеки та справедливості обробки персональної інформації. Модернізований Протокол CETS № 223 (Конвенція 108+) [2] адаптував ці положення до цифрової епохи, посиливши гарантії щодо транскордонного обміну даними та передбачивши створення незалежних наглядових органів. Стаття 14 Конвенції 108+ встановлює, що передача даних до інших держав можлива лише за умови наявності належних правових гарантій.

Вагомим доповненням до міжнародних стандартів стали Керівні принципи ОЕСР щодо захисту приватності та транскордонних потоків персональних даних (*OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*) [3], які визначають базові засади обробки даних: обмеження збору, пропорційність, безпека, відкритість та підзвітність.

Європейський підхід до приватності еволюціонував від Директиви 95/46/ЄС до Регламенту (ЄС) 2016/679 (GDPR) [4], який закріплює пріоритет приватності над економічною доцільністю. Згідно зі статтею 45 GDPR, передача даних до третіх країн дозволена лише за умови визнання Європейською Комісією «належного рівня захисту».

В Україні правове регулювання здійснюється на основі Закону «Про захист персональних даних» [5], гармонізованого відповідно до Конвенції 108 та GDPR. У 2022 р. Україна приєдналася до Протоколу CETS № 223, підтвердивши орієнтацію на європейські стандарти.

Нова редакція Закону передбачає створення незалежного органу – Національної комісії з питань захисту персональних даних, запровадження дієвих санкцій та чітких правил транскордонної передачі. Ці кроки є необхідними для визнання Україною статусу держави з «належним рівнем захисту» відповідно до статті 45 GDPR, що відкриває перспективу інтеграції до Єдиного цифрового ринку ЄС.

Верховний Суд у своїй практиці послідовно імплементує міжнародні стандарти захисту приватності у національне правозастосування. У постановках від 6 лютого 2025 р. у справах № 420/26651/23 [6] та № 420/14124/23 [7] Суд визнав правомірність використання Єдиного

державного демографічного реєстру та біометричних даних, зазначивши, що втручання у приватне життя є допустимим за умови дотримання принципу пропорційності та відповідності статті 8 Конвенції про захист прав людини і основоположних свобод.

Важливою складовою судової практики є також питання доступу до медичної інформації. У постанові від 11 листопада 2020 р. у справі № 442/4791/17 [8] Верховний Суд підтвердив, що право особи на отримання повної інформації про стан свого здоров'я є елементом права на приватність та захищається нормами цивільного, інформаційного та медичного законодавства. Відмова медичного закладу надати копії медичних документів була кваліфікована як порушення права на інформацію та права на захист персональних даних. Це рішення узгоджується з європейськими підходами до тлумачення статті 8 Конвенції про захист прав людини і основоположних свобод, згідно з якою право на приватне життя охоплює не лише заборону розголошення конфіденційних даних, а й позитивний обов'язок держави забезпечити особі доступ до інформації про стан її здоров'я.

Суд ЄС демонструє розширене тлумачення права на приватність у цифровому контексті. У справі *Lindenapothke* (C-21/23, 2024 р.) [9] він визнав, що навіть дані про замовлення безрецептурних ліків становлять інформацію про стан здоров'я, а отже, належать до категорії чутливих персональних даних і потребують посиленого захисту.

У справі *Meta Platforms Ireland v. EDPB* (T-319/24, 2025 р.) [10]. Суд розглянув модель «consent or pay» та підкреслив, що економічні інтереси не можуть переважати над вимогою вільної та усвідомленої згоди суб'єкта даних. Це рішення закріпило пріоритет автономії особи над комерційними практиками цифрових платформ.

У рішенні *Girginova v. Bulgaria* (№ 4326/18, 4 березня 2025 р.) [11] ЄСПЛ досліджував баланс між національною безпекою і відкритістю правосуддя. Суд встановив, що повна відмова журналісту в доступі до мотивувальної частини судового рішення становила непропорційне втручання в свободу вираження поглядів (стаття 10 Конвенції) і порушувала принципи публічності судового розгляду. ЄСПЛ наголосив, що навіть з міркувань державної безпеки держава має застосовувати менш інвазивні засоби, зокрема часткове закриття або редагування рішень.

Отже, право на приватність у цифрову добу зазнає якісної трансформації, виходячи за межі традиційного розуміння як особистого немайнового права та набуваючи міждисциплінарного виміру. У сучасних умовах центральним об'єктом його захисту стають персональні дані, що зумовлює зближення права на приватність із правом на захист персональної інформації. Саме тому механізми регулювання обробки персональних

даних розглядаються як ключова форма реалізації приватності у цифровому суспільстві.

Формування нормативної моделі захисту приватності визначається впливом міжнародних стандартів – Конвенції 108 та 108+, Загального регламенту ЄС (GDPR), Керівних принципів ОЕСР. У цих актах закріплюються базові принципи законності, пропорційності, підзвітності, прозорості та незалежного контролю обробки даних. У праві Європейського Союзу утверджено принцип, згідно з яким захист людської гідності та автономії особи превалює над економічними інтересами як держави, так і суб'єктів господарювання.

Національне законодавство України демонструє поступову гармонізацію з європейською правовою моделлю. Закон «Про захист персональних даних», приєднання України до Протоколу СЕТС № 223 та підготовка нової редакції закону із запровадженням незалежного органу з питань захисту даних свідчать про прагнення до імплементації стандартів ЄС. Водночас залишається низка системних викликів, серед яких – відсутність повноцінної функціонуючого наглядового органу, недостатня ефективність санкційного механізму та обмежене практичне застосування положень GDPR у національній правозастосовній діяльності.

Судова практика відіграє ключову роль у визначенні змісту права на приватність. Верховний Суд імплементує стандарти пропорційності та визнає право на доступ до медичної інформації як складову приватного життя, орієнтуючись на підходи ЄСПЛ. Суд ЄС розширює трактування персональних даних, відносячи до них навіть інформацію про придбання безрецептурних ліків, і наголошує, що згода на обробку даних має бути вільною, а не обумовленою економічним тиском. ЄСПЛ розвиває концепцію позитивних обов'язків держави у сфері приватності, підкреслюючи необхідність не лише утримання від втручання, а й забезпечення доступу до інформації та відкритості судового процесу, навіть за умов державної безпеки.

Водночас цифровізація посилює ризики масового спостереження, маніпулятивних технологій, алгоритмічної дискримінації та комерціалізації особистих даних. У цих умовах ефективна реалізація права на приватність можлива лише за умови системного, узгодженого з міжнародними стандартами правового регулювання, розвитку інституційного контролю, належного судового захисту та підвищення рівня цифрової обізнаності громадян.

Таким чином, приватність у цифрову добу перестає бути суто індивідуальним правом і набуває значення структурного елементу демократичної правової системи та довіри до цифрового середовища.

Література

1. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (1981 р.). URL: https://zakon.rada.gov.ua/laws/show/994_326
2. Протокол CETS № 223 до Конвенції № 108 (Конвенція 108+) «Про захист осіб щодо автоматизованої обробки персональних даних» від 18.05.2018 р. URL: https://zakon.rada.gov.ua/laws/show/994_363#Text
3. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 2001. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f/9789264196391-en.pdf
4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) / Європейський Парламент і Рада ЄС. URL: <https://gdpr-text.com/uk/>
5. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
6. Постанова Верховного Суду від 06 лютого 2025 року у справі № 420/26651/23 (провадження № К/990/16336/24). URL: <https://reyestr.court.gov.ua/Review/125011966>
7. Постанова Верховного Суду від 06 лютого 2025 року у справі № 420/14124/23 (провадження № К/990/15489/24). URL: <https://reyestr.court.gov.ua/Review/125011971>
8. Постанова Верховного Суду від 11 листопада 2020 року у справі № 442/4791/17 (провадження № 61-37882св18). URL: <https://reyestr.court.gov.ua/Review/93666639>
9. Court of Justice of the European Union. *Lindenapothke v Germany*, C-21/23: Judgment (Grand Chamber) of 4 October 2024. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=290696&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2925415>
10. General Court of the European Union. *Meta Platforms Ireland Ltd v European Data Protection Board*, справа T-319/24: Постанова (Десята палата) від 29.04.2025 р. URL: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=298762&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=200344>
11. *Girginova v. Bulgaria*, заява № 4326/18: Рішення Європейського суду з прав людини від 04.03.2025 р. URL: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-242053%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-242053%22]})