DOI https://doi.org/10.36059/978-966-397-557-3-1

ЦИФРОВА ЕПОХА ТА ПРАВО НА ПРИВАТНІСТЬ: ЕВОЛЮЦІЯ ЗАХИСТУ

Абдель Фатах А. С.
доктор філософії в галузі права, доцент,
доцент кафедри права,
Криворізький національний університет
м. Кривий Ріг, Україна

Право на приватність є фундаментальним правом людини, однак його суть і механізми захисту зазнали кардинальних змін з приходом цифрової ери. Технології, що стали невід'ємною частиною нашого життя – від збору даних вебсайтами до функціонування мобільних додатків – створили нові, безпрецедентні виклики для приватності. Масштаби, швидкість та характер обробки персональної інформації сьогодні незрівнянно вищі, ніж будь-коли в історії людства.

Стаття 8 Європейської конвенції з прав людини є основою захисту приватності, що гарантує право на недоторканність приватного та сімейного життя, житла й листування [1]. Завдяки гнучкому формулюванню Європейський суд з прав людини постійно адаптує її тлумачення до нових соціальних і технологічних викликів. Держава може вручатися лише за умови, що це передбачено законом і є необхідним у демократичному суспільстві – зокрема для безпеки, запобігання злочинам, охорони здоров'я, моралі чи прав інших осіб.

Практика Європейського суду з прав людини розкрила, що стаття 8 ЄКПЛ захищає чотири взаємопов'язані сфери: приватне життя – широке поняття, що охоплює фізичну, психологічну та моральну недоторканість, особистість автономії (зокрема щодо тіла та репродукції), конфіденційність даних, репутації й зображення, а також право на особистість стосунків; сімейне життя – яке гарантує захист родинних зв'язків між подружжями, батьками й дітьми та іншими близькими родичами; житло – яке забезпечує недоторканність дому та захист від незаконних обшуків чи втручань; і кореспонденція – що забезпечує конфіденційність будь-яких форм комунікації від несанкціонованого перехоплення [2].

Водночас стаття 8 не є абсолютною. Пункт 2 встановлює чіткі умови, за яких втручання з боку держави може бути визнане виправданим. Таке втручання має відповідати трьом критеріям: по-перше, втручання повинно мати підґрунтя у національному законодавстві, тобто передбачено законом. При цьому сам закон має бути «якісним»: доступним для громадян та передбачуваним у своєму застосуванні. Він також повинен містити належні

гарантії проти зловживань з боку влади; по-друге, втручання має переслідувати одну з легітимних цілей (законної мети) вичерпний перелік яких наведено у пункті 2 статті 8. Серед них – інтереси національної безпеки, запобігання злочинам, захист здоров'я чи моралі, а також захист прав і свобод інших осіб; по-третє, втручання має відповідати «нагальній суспільній потребі» та бути пропорційним до переслідуваної мети[2]. Держава повинна довести, що досягнення законної мети неможливе за допомогою менш обмежувальних заходів.

Ці фундаментальні принципи, сформовані в аналогову епоху для захисту від дій держави, виявилися занадто загальними, щоб дати відповідь на конкретні технічні та комерційні виклики, які принесла цифрова революція.

Окрім статті 8 ЄСПЛ Конвенція Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року та її Додатковий протокол від 8 листопада 2001 року є фундаментальними міжнародними актами у сфері захисту приватності. Конвенція встановлює загальні стандарти захисту прав і свобод фізичних осіб під час автоматизованої обробки їхніх персональних даних, зокрема регулює збір, зберігання, використання та можливість розголошення особистої інформації, забезпечуючи реалізацію права на приватне життя, закріпленого статтею 8 ЄКПЛ. Додатковий протокол посилює ці гарантії, вводячи обов’язковість створення незалежних органів нагляду за дотриманням законодавства про дані та встановлюючи правила щодо транскордонного обміну персональними даними, щоб забезпечити збереження рівня захисту після навіть захисту передачі інформації за межі національної юрисдикції [3; 4].

Закон України «Про захист персональних даних» від 1 червня 2010 року, є ключовим національним актом, який імплементує міжнародні стандарти захисту приватного життя, зокрема вимоги Статті 8 ЄКПЛ. Основним органом нагляду за дотриманням закону є Уповноважений Верховної Ради України з прав людини, який розглядає скарги, проводить перевірку, надає доступ до інформації та надає обов’язкові приписи [5]. Захист прав суб'єктів даних забезпечується через судову систему: суди можуть накласти штрафи, зупинити незаконну обробку даних або наказати видалення неправомірно зібраної інформації, що разом створює ефективний механізм контролю та відповідальності у сфері обробки персональних даних.

Однак, стрімкий розвиток цифрових технологій створив безпрецедентні виклики для традиційного розуміння приватності. Масштаби, швидкість та автоматизований характер збору персональних даних у цифрову епоху вимагали нової, більш детальної та превентивної правової відповіді для регулювання нових технологічних реалій. Сучасний бізнес та ІТ-продукти обробляють величезні масиви персональних даних, створюючи нові ризики для приватності. Зокрема, інтернет-магазини збирають імена, адреси

доставки, номери телефонів та електронні пошти клієнтів з ЄС. Цей процес виходить далеко за межі традиційного поняття «кореспонденції», створюючи централізовані бази даних, вразливі до витоків та зловживань. Такі технології, як IP-адреси, cookie-файли та дані про геолокацію, дозволяють створювати детальні цифрові «портрети» користувачів є новою формою спостереження, що дозволяє відстежувати поведінку, інтереси та звички людей у небачених раніше масштабах. Натомість, додатки, доступні для користувачів з ЄС через App Store чи Google Play, часто збирають широкий спектр даних – від списку контактів до даних про місцезнаходження, причому користувачі не завжди чітко розуміють мету та обсяг такого збору.

В рамках Європейського співтовариства ці нові реалії зумовили появу Загального регламенту про захист даних (далі – GDPR), що набув чинності в ЄС у 2018 році, став найповнішою та найсуворішою у світі законодавчою ініціативою у сфері захисту даних, розробленою спеціально для цифрової ери. Його головна мета – повернути громадянам контроль над їхніми персональними даними та уніфікувати правила їх обробки на всій території Європейського Союзу. GDPR надає дуже широке визначення персональних даних – це будь-яка інформація, яка прямо або опосередковано дозволяє ідентифікувати живу особу. До них належать лише традиційні дані, як-от ім'я, ім'я чи номер телефону, а й цифрові сліди: IP-адреси, cookie-файли, геолокація, електронна пошта, фотографії, відеозаписи, а також чутливі категорії даних – біометрична, медична інформація, відомості про релігійні переконання, політичні погляди чи сексуальну орієнтацію [5].

Ключова особливість GDPR – його екстериторіальна дія: регламент поширюється на будь-яку організацію у світі, якщо він обробляє дані осіб, які перебувають на території ЄС. Це означає, що українські компанії – будь то інтернет-магазини, SaaS-платформи чи готелі, що обслуговують європейських клієнтів – зобов'язані виконувати його вимоги. Основу регулювання становлять сім принципів законної обробки даних: законність, справедливість і прозорість; обмеження мети; мінімізація даних; точність; обмеження терміну зберігання; цілість і конфіденційність; а також підзвітність [5]. Вони спрямовані на запобігання посиленому збору, прихованому використанню та довгостроковому зберіганню даних без необхідності.

Окрім обов'язків для бізнесу, GDPR надає суб'єктам даних широкий спектр прав: право на інформацію, доступ до власних даних, їх виправлення або повного видалення («право на забуття»), обмеження обробки, перенесення даних, перетворення проти обробки та захист від автоматизованих рішень, зокрема профілювання [5]. Ці механізми разом забезпечують реальний контроль людей над вашою цифровою ідентичністю. Відповідність цим принципам та забезпечення прав

користувачів, особливо в IT-сфері, вимагає не лише юридичних консультацій, а й глибоких технічних та архітектурних рішень на рівні продукту.

Для IT-компаній та розробників GDPR – це не лише набір юридичних правил, а й технічна філософія, що має бути інтегрована в сам процес створення продукту від його зародження. Регламент вимагає проактивного підходу до захисту даних, а не реактивного реагування на проблеми.

У реалізації ключової ролі GDPR діють два принципи: «приватність через проектування» та «приватність за замовчуванням». Перший вимагає інтегрувати захист даних ще на етапі розробки продукту – з шифруванням, псевдонімізацією та технічною підтримкою прав користувачів, зокрема «права на забуття». Другий передбачає, що всі налаштування конфіденційності мають бути максимально захищеними одразу, а додатковий збір даних – наприклад, для аналітики чи маркетингу – активується лише після свідомої згоди користувача [5]. Використання сторонніх сервісів (Google Analytics, Mailchimp, AWS тощо) не заборонено, але вимагає від компанії як контролера даних підписання угод про обробку, налаштування анонімізації, подвійного підтвердження згоди та прозорої інформації. Таким чином, приватність стає не лише юридичною вимогою, але й невід'ємною частиною якості продукту та користувацького досвіду.

Хоча Україна не є членом ЄС, дотримання GDPR є критично важливим для українських компаній, які працюють з європейським ринком. GDPR має екстериторіальний характер – він поширюється на будь-яку організацію поза ЄС, якщо він обробляє персональні дані осіб, які перебувають у ЄС. Це стосується інтернет-магазинів, IT-сервісів, SaaS-платформ, готелів, аутсорсингових компаній тощо, які мають клієнтів, користувачів або партнерів у Європі.

Недотримання GDPR може призвести до серйозних наслідків: від блокування доступу до європейського ринку та втрати довіри клієнтів до штрафів (за наявності юридичного представництва в ЄС) або припинення співпраці з європейськими партнерами. Крім того, впровадження стандартів GDPR забезпечує рівень кібербезпеки, перевірки користувачів і конкурентоспроможності українських продуктів на глобальному ринку.

Висновки. Захист приватності еволюціонував від загальних норм (стаття 8 ЄКПЛ) до конкретних, технічно орієнтованих вимог GDPR, які вважають не лише те, що захищати, а й як це робити в цифрову епоху. Для бізнесу відповідність GDPR – це не тільки юридична умова України, а й ознака надійності та конкурентних переваг на глобальному ринку. Ефективний захист даних вимагає поєднання правових норм, технічної відповідальності та культури поваги до приватності всередині компаній і суспільства.

Література

1. Конвенція про захист прав людини і основоположних свобод: Конвенція Ради Європи від 04.11.1950 : станом на 1 серп. 2021 р. URL: https://surl.li/cacuoe (дата звернення: 16.10.2025).
2. Article 8 – Right to respect for private and family life – ЄСПЛ-KS – Knowledge Sharing. ЄСПЛ-KS. URL: https://surl.li/zbjnvb (дата звернення: 16.10.2025).
3. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28.01.1981: станом на 6 лип. 2010 р. URL: https://surl.li/mdtjrr (дата звернення: 16.10.2025).
4. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Протокол Ради Європи від 08.11.2001 : станом на 6 лип. 2010 р. URL: https://surl.li/wilbgg (дата звернення: 16.10.2025).
5. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://surli.cc/ivlffs (дата звернення: 16.10.2025).
6. Regulation – 2016/679 – EN – gdpr – EUR-Lex. EUR-Lex – Access to European Union law – choose your language. URL: https://surl.lt/pzwoir (date of access: 16.10.2025).

DOI https://doi.org/10.36059/978-966-397-557-3-2

AI ACT ЯК ПРАВОВИЙ СТАНДАРТ ЕТИЧНОГО ШІ: ІМПЛЕМЕНТАЦІЙНІ ВИКЛИКИ ДЛЯ УКРАЇНСЬКОГО ЗАКОНОДАВСТВА

Бородін К. С.
викладач кафедри загальнотеоретичних правових і соціально-гуманітарних дисциплін,
Київський університет права Національної академії наук України
м. Київ, Україна

Стрімкий розвиток моделей штучного інтелекту (ШІ) створює фундаментальні виклики для правової системи, особливо в аспекті дотримання прав людини та етичних стандартів. У відповідь на ці виклики Європейський Союз (ЄС) розробив регламент про штучний інтелект **Artificial Intelligence Act** (AI Act) – перший комплексний нормативно-правовий акт, який встановлює чітку систему ризик-орієнтованого