САДКОВСЬКИЙ С. П.,
аспірант кафедри галузевого права
та загальноправових дисциплін
*(Заклад вищої освіти «Відкритий
міжнародний університет розвитку
людини «Україна»)*

УДК 347.77:004(4+477)
DOI https://doi.org/10.32842/2078-3736/2025.5.2.9

ЦИВІЛЬНО-ПРАВОВА ВІДПОВІДАЛЬНІСТЬ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ДОСВІД ЄС ТА ПЕРСПЕКТИВИ ДЛЯ УКРАЇНИ

У цій статті здійснено порівняльно-правовий аналіз законодавчого регулювання цивільно-правової відповідальності у сфері інформаційних технологій у державах Європейського Союзу.

Особливу увагу приділено застосуванню основних положень Загального регламенту про захист даних (GDPR) як правової основи для встановлення відповідальності за порушення у цифровому середовищі та їх значення в контексті сучасного інформаційного суспільства. Розглянуто правові засади обробки персональних даних, зокрема принципам законності, прозорості, цільової обмеженості та мінімізації даних. Проаналізовано механізми захисту прав суб'єктів персональних даних, включаючи право на доступ, виправлення, стирання та заперечення проти обробки даних. У фокусі також перебувають обов'язки контролерів та операторів персональних даних, а також роль органів з нагляду.

Проведено порівняльний аналіз із законодавством України у сфері захисту персональних даних, акцентуючи на відмінностях у правозастосовній практиці та напрямках гармонізації національного права з європейськими стандартами. Підкреслено необхідність удосконалення українського законодавства в умовах цифрової трансформації та інтеграції до правового простору ЄС. Дослідження ґрунтується на нормативних джерелах Європейського Союзу, судовій практиці, а також наукових працях європейських та українських правників.

Окреслено особливості національних правових систем окремих держав-членів ЄС, зокрема Німеччини, Франції, Італії, Іспанії та Польщі.

Запропоновано напрями вдосконалення українського законодавства з урахуванням європейських практик. Наукова праця має на меті поглибити розуміння тенденцій формування ефективної моделі цивільно-правової відповідальності в сфері інформаційних технологій та сприяти імплементації кращих практик у національну правову систему.

Наголошено, що цифровізація суспільства та зростаюча роль інформаційних технологій у всіх сферах життя зумовили необхідність удосконалення правового регулювання, зокрема в частині встановлення цивільно-правової відповідальності за правопорушення у сфері ІТ. Для України, яка орієнтована на європейський вектор розвитку, особливо актуальним є вивчення іноземного досвіду законодавчого регулювання відповідальності у сфері інформаційних технологій.

Ключові слова: *цивільно-правова відповідальність, інформаційні технології, GDPR, Європейський Союз, захист персональних даних, Цивільний кодекс України, Закон України «Про захист персональних даних».*

Sadkovskyi S. P. Civil liability in the field of information technology: EU experience and prospects for Ukraine

This article presents a comparative legal analysis of legislative regulation of civil liability in the field of information technology in the European Union Member States.

Special attention is given to the application of the core provisions of the General Data Protection Regulation (GDPR) as the legal basis for establishing liability for violations in the digital environment and their significance in the context of the modern information society. The legal foundations of personal data processing are examined, including the principles of lawfulness, transparency, purpose limitation, and data minimization. Mechanisms for the protection of data subjects' rights, such as the right to access, rectification, erasure, and objection to data processing, are analyzed. The obligations of data controllers and processors, as well as the role of supervisory authorities, are also in focus.

A comparative analysis with the legislation of Ukraine in the field of personal data protection is conducted, emphasizing differences in law enforcement practices and directions for harmonizing national law with European standards. The need to improve Ukrainian legislation in the context of digital transformation and integration into the EU legal space is highlighted. The study is based on regulatory sources of the European Union, case law, as well as scientific works of European and Ukrainian legal scholars.

The article outlines the specific features of national legal systems of selected EU Member States, including Germany, France, Italy, Spain, and Poland.

Recommendations are proposed for improving Ukrainian legislation with regard to European best practices. This scholarly work aims to deepen the understanding of trends in the formation of an effective model of civil liability in the field of information technology and to promote the implementation of best practices into the national legal system.

It is emphasized that the digitalization of society and the growing role of information technologies in all spheres of life have made it necessary to improve legal regulation, particularly in establishing civil liability for IT-related violations. For Ukraine, which is oriented towards the European development vector, the study of foreign legislative experience in this area is of particular relevance.

Key words: *civil liability, information technologies, GDPR, European Union, personal data protection, Civil Code of Ukraine, Law of Ukraine "On Personal Data Protection".*

Вступ. Цифровізація суспільства та зростаюча роль інформаційних технологій у всіх сферах життя зумовили необхідність удосконалення правового регулювання, зокрема в частині встановлення цивільно-правової відповідальності за правопорушення у сфері інформаційних технологій. У Європейському Союзі сформовано єдину правову платформу для захисту персональних даних та забезпечення належного рівня відповідальності в цифровому середовищі – насамперед, через застосування положень Загального регламенту про захист даних (GDPR). Водночас реалізація положень GDPR у національних законодавствах різниться за формами та підходами.

Для України, яка орієнтована на європейський вектор розвитку, особливо актуальним є вивчення іноземного досвіду законодавчого регулювання відповідальності у сфері інформаційних технологій. Сучасне українське законодавство лише формує ефективні механізми цивільно-правового реагування на порушення цифрових прав, що потребує наукового аналізу, порівняння з кращими європейськими практиками та вироблення рекомендацій щодо подальшої гармонізації національного права.

Аналіз останніх досліджень та публікацій. Проблематика правового регулювання відповідальності у сфері інформаційних технологій є предметом пильної уваги науковців

як в Україні, так і в країнах Європейського Союзу. Зокрема, у працях таких дослідників, як К. Кьорнер, П. Де Херт, акцент зроблено на необхідності збалансування права на приватність та цифрових інновацій, а також на ефективності правозастосовних механізмів у межах ЄС.

В українському правознавстві помітним є внесок науковців О. Тищенко, О. Шимків, які досліджують цивільно-правові аспекти цифровізації, правовий режим персональних даних, а також виклики для правозастосування в умовах стрімкого розвитку технологій. Окремі публікації присвячено порівняльному аналізу норм GDPR та українського законодавства про захист персональних даних, зокрема у працях М. Головатого.

Разом з тим, незважаючи на наявність теоретичних напрацювань, питання цивільно-правової відповідальності за порушення у сфері інформаційних технологій, у тому числі за неправомірну обробку персональних даних, потребує подальшого дослідження.

Постановка завдання. Сучасний розвиток інформаційних технологій зумовлює трансформацію правової системи, зокрема в частині регулювання відповідальності за правопорушення у цифровому середовищі. Цивільно-правова відповідальність у сфері інформаційних технологій набуває особливого значення в умовах масового обміну даними, автоматизації процесів та зростання ризиків для приватних осіб і бізнесу.

Водночас в Україні спостерігається фрагментарність правового регулювання у цій сфері, що ускладнює ефективний захист прав суб'єктів цифрових правовідносин. У зв'язку з цим особливої актуальності набуває вивчення зарубіжного досвіду, зокрема законодавства держав-членів Європейського Союзу, яке вже пройшло етап адаптації до реалій цифрової епохи.

Метою статті є здійснення порівняльно-правового аналізу законодавства країн ЄС щодо цивільно-правової відповідальності у сфері інформаційних технологій, а також визначення можливостей застосування окремих європейських підходів у контексті українського законодавства.

Результати дослідження. Нині, на тлі загальноєвропейських тенденцій українське законодавство у сфері інформаційних технологій, зокрема в частині цивільно-правової відповідальності, все ще перебуває у процесі становлення та адаптації. Попри наявність окремих норм у Цивільному кодексі України [13], Законі України «Про захист персональних даних» [9], а також у проєкті Закону «Про захист персональних даних» (який має на меті гармонізацію з GDPR) [10], загальна система правового захисту постраждалих осіб від негативного впливу інформаційних технологій є фрагментарною та недостатньо ефективною.

На нашу думку для чіткого розуміння питання щодо гармонізації українського законодавства до загальноєвропейського, необхідно більш ретельно розглянути та проаналізувати Положення GDPR (General Data Protection Regulation).

Положення GDPR (General Data Protection Regulation) – це ключові нормативні вимоги Загального регламенту Європейського Союзу про захист персональних даних, який набув чинності 25 травня 2018 року. Він був ухвалений Європейським Союзом та набув чинності у 2016 році та повноцінно почав застосовуватись лише у травні 2018 року [7].

GDPR є основним нормативно-правовим актом, що регулює обробку персональних даних у ЄС, і застосовується як до європейських компаній, так і до іноземних організацій, які обробляють дані громадян ЄС. До основних положень GDPR, що стосуються обробки даних і встановлення відповідальності можемо віднести такі:

1. Стаття 5 – Принципи обробки персональних даних – встановлює основні засади, за якими дозволено збирати, зберігати та використовувати персональні дані:

- законність, справедливість і прозорість – дані мають оброблятись на законних підставах, чесно та зрозуміло для суб'єкта;
- цільове обмеження – дані збирають лише для чітко визначених і законних цілей;
- мінімізація даних – лише ті дані, що дійсно необхідні;
- точність – дані мають бути актуальними й точними;
- обмеження зберігання – не довше, ніж потрібно для мети обробки;

– цілісність і конфіденційність – захист від несанкціонованого доступу або втрати;
– підзвітність – відповідальність за дотримання усіх цих принципів несе контролер даних.

2. Статті 12–22 – Права суб'єкта персональних даних, гарантують громадянам ЄС контроль над своїми даними:
– ст. 12 – інформування – компанія повинна прозоро повідомляти, як і для чого збирає дані;
– ст. 13–14 – обов'язок надавати інформацію при зборі даних – прямо або через третіх осіб;
– ст. 15 – право доступу – особа може отримати копію своїх даних;
– ст. 16 – право на виправлення – якщо дані неточні або неповні;
– ст. 17 – право на стирання («право бути забутим») – коли обробка даних більше не має законних підстав;
– ст. 18 – право на обмеження обробки – наприклад, під час перевірки точності даних;
– ст. 20 – право на перенесення даних – можливість отримати свої дані в машиночитаному форматі;
– ст. 21 – право на заперечення – наприклад, проти обробки в рекламних цілях;
– ст. 22 – автоматизоване прийняття рішень – заборона рішень без участі людини, якщо вони мають істотний вплив.

3. Стаття 24–25 – Відповідальність контролера та принцип «Privacy by design»:
– ст. 24 – контролер має не лише дотримуватись GDPR, але й бути здатним довести це (підзвітність);
– ст. 25: принципи Privacy by Design і by Default – системи повинні бути спроектовані так, щоб забезпечити максимальний захист особистих даних з самого початку.

4. Статті 33–34 – Повідомлення про порушення.
– ст. 33 – у разі витоку персональних даних – контролер зобов'язаний протягом 72 годин повідомити наглядовий орган;
– ст. 34 – якщо порушення може призвести до високого ризику для суб'єкта – потрібно також повідомити саму особу.

5. Статті 83–84 – Штрафи та санкції:
– ст. 83 – визначає розміри адміністративних штрафів: – до 10 млн євро або 2% річного обороту – за порушення загального характеру; – до 20 млн євро або 4% обороту – за грубі порушення, як-от ігнорування прав суб'єктів;
– ст. 84 – країни-члени можуть вводити додаткову цивільно-правову та кримінальну відповідальність за порушення регламенту [11].

Однак, на нашу думку під час дослідження необхідно виконати також порівняльну характеристику цивільно-правової відповідальності у сфері інформаційних технологій в країнах Європейського Союзу.

Отже, у межах Європейського Союзу законодавство у сфері інформаційних технологій регулюється як на рівні загальносоюзного права (зокрема, Регламентом GDPR), так і національними нормативними актами. Хоча всі країни ЄС імплементували положення GDPR, механізми цивільно-правової відповідальності та практика їх застосування мають певні відмінності.

У Німеччині питання відповідальності за порушення у сфері обробки персональних даних регулюється Федеральним законом про захист даних (BDSG), який імплементує GDPR. Закон прямо передбачає право на компенсацію за матеріальні та нематеріальні збитки (ст. 82 GDPR). У країні діє чітка судова практика, що демонструє суворе тлумачення обов'язків контролера та обробника даних.

Франція реалізує вимоги GDPR через оновлений Закон «Про інформацію і свободи» («Loi Informatique et Libertés»). Законодавство дозволяє подавати цивільні позови навіть у випадках етичних порушень, зокрема за відсутності згоди на обробку персональних даних.

Національний орган з питань захисту даних – CNIL – активно застосовує санкції, включаючи фінансові стягнення.

В Італії Кодекс захисту персональних даних (Legislative Decree No. 196/2003, у редакції після GDPR) передбачає презумпцію вини контролера даних, а також можливість стягнення компенсації за моральну шкоду. У країні діють спеціалізовані суди, які розглядають спори у сфері IT [3].

Іспанія має Закон № 3/2018 про захист персональних даних, що уточнює процедури притягнення до відповідальності за порушення обов'язків контролера та обробника даних. Відшкодування може бути надане як за сам факт порушення, так і за неналежне інформування суб'єкта даних. Контролюючий орган AEPD демонструє активну правозастосовну практику [1].

У Нідерландах Закон про виконання GDPR (UAVG) передбачає можливість колективних позовів, а також чітко прописані механізми компенсації шкоди через суд. Країна має розвинену систему кіберстрахування та цифрового арбітражу, що слугує інструментом додаткового регулювання ризиків [6].

Польське законодавство з 2018 року також імплементує GDPR, визначаючи чіткі підстави для цивільного позову при порушенні обов'язків з обробки персональних даних. Спостерігається зростання кількості кейсів, пов'язаних із витоками персональної інформації, що підвищує значущість цивільно-правової відповідальності в цій сфері [7].

Австрія у своєму Законі про захист даних (Datenschutzgesetz – DSG) визнає право на компенсацію нематеріальної шкоди як окрему форму відповідальності. Закон також дозволяє групові позови, що розширює можливості суб'єктів даних для захисту своїх прав [5].

У Швеції Закон про доповнення до GDPR передбачає застосування цивільної відповідальності лише за умови доведення конкретної шкоди. Держава дотримується ліберального підходу у втручанні у відносини сторін, віддаючи перевагу договірному врегулюванню.

Чеська Республіка ухвалила Закон № 110/2019 Sb., який визначає порядок обробки персональних даних відповідно до GDPR. Механізми відповідальності базуються на положеннях Громадянського кодексу та Регламенту. В країні активно впроваджується практика альтернативного врегулювання спорів (ADR).

Що стосується наприклад Греції, то Закон № 4624/2019 визначає як адміністративну, так і цивільну відповідальність за порушення прав суб'єктів персональних даних. Окрему роль у забезпеченні реалізації прав відіграє Омбудсмен з питань захисту даних.

Аналіз національних правових підходів країн Європейського Союзу до регулювання цивільно-правової відповідальності у сфері інформаційних технологій демонструє загальну тенденцію до гармонізації правозастосовної практики на основі положень GDPR, однак виявляє й суттєві відмінності у реалізації цих норм.

Зокрема, такі країни, як Німеччина, Франція, Італія демонструють високий рівень нормативної деталізації, наявність сформованої судової практики та суворий контроль за дотриманням вимог щодо обробки персональних даних. У цих юрисдикціях активно застосовуються механізми компенсації як матеріальної, так і нематеріальної шкоди, а також діють спеціалізовані судові інституції або незалежні регулятори з широкими повноваженнями [8].

У країнах на кшталт Нідерландів, Австрії, Польщі, акцент робиться на спрощенні доступу до правосуддя, можливості колективного захисту інтересів, а також розвитку альтернативних способів компенсації шкоди, зокрема через механізми кіберстрахування або цифрового арбітражу.

Скандинавські країни (зокрема Швеція) застосовують більш гнучкий і поміркований підхід, зосереджуючись на договірних практиках, високих стандартах прозорості та вимогах до фіксації фактичної шкоди. Вищезазначене дозволяє забезпечити баланс між правами суб'єктів даних та інтересами бізнесу.

У свою чергу, центрально- і східноєвропейські держави (Польща, Чехія, Греція) ще формують сталу правозастосовну практику, однак впевнено імплементують ключові

положення GDPR, поступово адаптуючи західноєвропейські моделі відповідальності до національних умов.

Загалом, можна зробити висновок, що ефективність цивільно-правової відповідальності у сфері інформаційних технологій у країнах ЄС прямо залежить від ступеня інституційної зрілості правової системи, активності наглядових органів і наявності реального доступу до правосуддя. Їх досвід є надзвичайно цінним для країн, які перебувають на шляху до вдосконалення власної правової бази у сфері цифрових відносин, зокрема для України [4].

Найбільшими проблемами залишаються відсутність чіткої процедури визначення шкоди у цифровому середовищі, складність доведення причинно-наслідкового зв'язку, а також відсутність єдиного наглядового органу з широкими повноваженнями у сфері захисту персональних даних, подібного до європейських Data Protection Authorities (DPA). Крім того, українська судова практика у цій сфері досі є нечисельною, що створює правову невизначеність для сторін [12].

Проведений аналіз європейського досвіду демонструє доцільність імплементації в Україні таких підходів:

− розширення переліку видів шкоди, які підлягають компенсації (включно з нематеріальною/моральною);

− запровадження механізму колективних позовів у разі масових порушень прав споживачів або користувачів цифрових послуг;

− інституціональне посилення повноважень Уповноваженого ВРУ з прав людини або створення спеціального наглядового органу, подібного до CNIL (Франція) чи AEPD (Іспанія);

− спрощення процедур доказування у справах, пов'язаних з інформаційними технологіями, зокрема за рахунок експертної оцінки електронних доказів [14].

Впровадження зазначених механізмів дозволить створити більш ефективну модель цивільно-правового захисту осіб у цифровому середовищі, підвищити рівень правової визначеності та стимулювати цифрову трансформацію із дотриманням принципів прав людини.

Висновки. Отже, проведене дослідження засвідчує, що законодавство країн Європейського Союзу у сфері цивільно-правової відповідальності за порушення в IT-середовищі ґрунтується на положеннях GDPR та розвиненій національній практиці, яка забезпечує високий рівень захисту прав суб'єктів персональних даних. Водночас, попри гармонізацію на рівні ЄС, підходи до реалізації цих положень у різних країнах залишаються варіативними, що обумовлено особливостями правових систем, інституційного забезпечення та судової практики.

Для України особливо важливо вивчати ці моделі в умовах цифрової трансформації та наближення до європейських стандартів. Аналіз показав, що українська правова система лише формує ефективні інструменти цивільно-правової відповідальності сфері інформаційних технологій, тому запозичення окремих інституцій (зокрема механізму компенсації нематеріальної шкоди, колективних позовів, функціонування спеціалізованих регуляторів) є не лише актуальним, а й необхідним.

Впровадження комплексного, системно інтегрованого підходу до правового захисту у цифровому середовищі дозволить Україні не лише забезпечити належний рівень гарантій для своїх громадян, а й сприятиме розвитку цифрової економіки, з урахуванням принципів верховенства права, технологічної нейтральності та захисту основоположних прав.

Список використаних джерел:

1. Albrecht J.P. How the GDPR will change the world. European Data Protection Law Review, 2016. Vol. 2(3). P. 287–289.

2. Bygrave L. A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014. 448 p.

3. De Hert P., Papakonstantinou V. The proposed Data Protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. Computer Law & Security Review. 2012. Vol. 28. P. 130–142.

4. Kuner C. Transborder Data Flows and Data Privacy Law. Oxford: Oxford University Press, 2020. 416 p.

5. Telemediengesetz (TMG): Bundesrepublik Deutschland. URL: https://www.gesetze-im-internet.de/tmg/.

6. Weber R.H. Internet of Things – New security and privacy challenges. Computer Law & Security Review, 2010. Vol. 26(1). P. 23–30.

7. Головатий Н.Т. Правове регулювання захисту персональних даних: GDPR та законодавство США, Канади й України. *Науковий вісник Ужгородського національного університету,* 2024. Вип. 85: ч. 2. С. 288-292. DOI: https://doi.org/10.24144/2307-3322.2024.85.2.42.

8. Копилов О. В. Інформаційне право: підручник. Київ: Юрінком Інтер, 2019. 512 с.

9. Про захист персональних даних. Закон України № 2297-VI від 01.06.2010. URL: https://zakon.rada.gov.ua/laws/show/2297-17/ed20100601#Text.

10. Проект Закону про захист персональних даних. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707.

11. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 р. про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний обіг таких даних (Загальний регламент про захист даних, GDPR). URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

12. Тищенко О. І. Цивільно-правова відповідальність у сфері інформаційних технологій. *Підприємництво, господарство і право,* 2021. № 3. С. 72–76.

13. Цивільний кодекс України: Закон України від 16.01.2003 № 435-IV. *Відомості Верховної Ради України*. 2003. № 40–44. Ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text.

14. Шимків О. Ю. Правові аспекти цифрової відповідальності в Україні та ЄС. *Інформація і право,* 2020. № 2. С. 45–50.

Дата першого надходження рукопису до видання: 03.09.2025
Дата прийнятого до друку рукопису після рецензування: 24.10.2025
Дата публікації: 28.11.2025