УДК 339.9
JEL Classification: K24; K33; O38; L86

ЄВРОПЕЙСЬКИЙ ДОСВІД ІНСТИТУЦІОНАЛІЗАЦІЇ ЗАХИСТУ ДАНИХ

©2025 **КОРНІВСЬКА В. О.**

УДК 339.9
JEL Classification: K24; K33; O38; L86

Корнівська В. О.

Європейський досвід інституціоналізації захисту даних

Метою цієї статті є висвітлення європейського досвіду інституціоналізації захисту даних, аналіз особливостей правозастосування окремих норм Загального регламенту про захист даних, на цій основі – характеристика ефективності європейського правового поля. Результати дослідження показали, що створення умов для ефективного правозастосування законодавства щодо захисту даних залежить від багатьох факторів геоекономічного, геополітичного та інституційного характеру. На сьогодні правозастосування є обмежено ефективним через укорінення глобально-монополістичної інформаційної асиметрії, - інформаційного домінування корпорацій над їх користувачами внаслідок використання переваг володіння передовими технологіями збору, систематизації інформації в економічних та соціогуманітарних цілях корпорацій. Умови глобально-монополістичної інформаційної асиметрії створюватимуть додатковий тиск на діяльність пересічних суб'єктів інформаційного простору через зростання невизначеності. У статті підкреслено необхідність імплементації європейського законодавства в українських правових координатах, формування відповідних наглядових структур. Водночас показано, що захист даних прийматиме дедалі конфліктніший характер, що зумовлено особливостями форм власності у цифровій економіці. На цьому тлі необхідною є правова воля і рішучість держави діяти у контексті захисту прав найуразливішої частини суб'єктів інформаційного простору – користувачів.

Ключові слова: *інституціоналізація захисту даних, законодавство ЄС, глобальні інформаційні гіганти, глобально-монополістична інформаційна асиметрія.*

DOI: *https://doi.org/10.32983/2222-0712-2025-3-28-36*

Табл.*: 1.* ***Бібл.:*** *33.*

Корнівська Валерія Олегівна *– доктор економічних наук, старший науковий співробітник відділу економічної теорії, Інститут економіки та прогнозування НАН України (вул. Панаса Мирного, 26, Київ, 01011, Україна)*

E-mail: *vkornivska@ukr.net*

ORCID: *https://orcid.org/0000-0002-0348-0404*

UDC 339.9
JEL Classification: K24; K33; O38; L86

Kornivska V. O. The European Experience of Institualizing the Data Protection

The aim of this article is to highlight the European experience of institutionalizing the data protection, analyze the specifics of the application of certain provisions of the General Data Protection Regulation, and on this basis, characterize the efficiency of the European legal framework. The results of the research showed that creating conditions for the efficient enforcement of data protection legislation depends on many factors of a geo-economic, geopolitical, and institutional nature. Currently, enforcement is limitedly efficient due to the entrenchment of globally monopolistic information asymmetry – the informational dominance of corporations over their users as a result of advantages gained from possessing advanced technologies for collecting and systematizing information for the economic and socio-humanitarian purposes of corporations. The conditions of global monopolistic information asymmetry will create additional pressure on the activities of ordinary subjects in the information space due to the increasing uncertainty. The article emphasizes the necessity of implementing European legislation within the Ukrainian legal framework and forming appropriate supervisory structures. Also, it is shown that data protection will take on an increasingly conflicted nature, driven by the peculiarities of ownership forms in the digital economy. Against this backdrop, the legal will and determination of the state to act in the context of protecting the rights of the most vulnerable users in the information space is essential.

Keywords: *institutionalization of data protection, EU legislation, global information giants, global monopolistic information asymmetry.*

Tabl.: *1.* ***Bibl.:*** *33.*

Kornivska Valeriia O. *– Doctor of Sciences (Economics), Senior Research Fellow of the Department of Economic Theory, Institute for Economics and Forecasting of NAS of Ukraine (26 Panasa Myrnoho Str., Kyiv, 01011, Ukraine)*

E-mail: *vkornivska@ukr.net*

ORCID: *https://orcid.org/0000-0002-0348-0404*

Вступ. У 2020 році Міністерством цифрової трансформації одним із пріоритетних напрямків галузевої інтеграції з ЄС було визначено наближення України до єдиного цифрового ринку Європейського Союзу [1].

Формування єдиного цифрового ринку ЄС розпочалося у 2015 році зі створення технологічних, інституційних та економічних умов для спрощення транскордонної онлайн-торгівлі. На цьому шляху вже у 2016 та 2017 роках відбувся ряд знакових подій, що сприяли досягненню поставлених цілей: припинення плати за роумінг; модернізація захисту даних; врегулювання транскордонного руху онлайн-контенту; угода про розблокування електронної

комерції шляхом припинення невиправданого геоблокування [2].

Сьогодні триває налаштування європейського інституційного середовища для активізації цифровізації як ключової стратегії довгострокового розвитку. При цьому вважається, що вибудовування єдиного цифрового ринку зробить цифровий перехід найбільш гармонійним та ефективним як у контексті досягнення цілей національних держав, так і у частині підтримки необхідного рівня конкурентоспроможності та впливу ЄС на міжнародній арені у процесі цифрового переходу. Практика показує, що у сфері інституціоналізації цифрових трансформацій та розбудови цифрового суспільства ЄС знаходиться в авангарді законотворчого процесу для оптимізації технологічного, економічного, соціального та гуманітарного розвитку.

У сучасних умовах подальшої реалізації євроінтеграційного курсу України важливо усвідомити, що формування єдиного цифрового ринку ЄС триває вже практично десять років, і сьогодні є тенденції європейського розвитку, до яких ми маємо бути готовими, є досвід, який буде для нас корисним, і є ризики, які ми маємо враховувати, беручи до уваги ключові характеристики інституційного середовища, до якого ми прагнемо приєднатися.

Формування інституційного середовища оперування даними в умовах цифрового суспільства приймає дедалі конфліктніший характер, що зумовлено особливостями форм власності у цифровій економіці, у якій, як доводить академік А. Гриценко, відбувається діалектичний збіг індивідуальної та всезагальної (суспільної) форм [3]. Водночас процеси інституціоналізації захисту даних розвиваються на основі домінування принципів індивідуального привласнення, що зумовлює дисбаланси та сум'яття в інформаційному просторі. Це, зокрема, проявляється у тому, що, задаючи глобальний інституційний тон щодо захисту даних, ЄС все частіше демонструє прецеденти конфліктів та обмеженої інституційної ефективності в процесі правозастосування норм на перший погляд міцного законодавства.

Водночас у частині реалізації людиноцентричних мотивацій інституціоналізації захисту даних і первісної спрямованості відповідних інститутів на жорстке правозастосування кращих за європейські підходи у сфері захисту даних поки не існує. Тому вони сьогодні знаходяться під пильною увагою наукової спільноти. Проблематиці захисту даних в умовах зростаючих викликів цифрового переходу присвячені роботи Бикова О. М., Савченко В. В. [4], які, досліджуючи європейські стандарти захисту даних, вносять важливі пропозиції щодо створення відповідного інституційного середовища в Україні.

Практичні аспекти правового регулювання захисту даних в ЄС та в Україні висвітлені в роботі Бема М. та Городиського І [5]. Пилипчук В. Г., Брижко В. М. характеризують історичні спекти розвитку законодавства України у сфері захисту даних [6].

Baghal-Schmid A., Esser L. систематизують статистику, що демонструє ефективність правозастосування норм європейського законодавства у сфері захисту даних [7]. Jahangir R. розглядає спроби європейської лібералізації норм захисту даних [8].

Метою цієї статті є висвітлення європейського досвіду інституціоналізації захисту даних, аналіз особливостей правозастосування окремих норм Загального регламенту про захист даних, на цій основі характеристика ефективності європейського правового поля.

Викладення основного матеріалу дослідження. Захист фізичних осіб під час опрацювання персональних даних був визнаний фундаментальним правом ще задовго до формування європейського цифрового ринку. Статтею 8 (1) Хартії фундаментальних прав Європейського Союзу («Хартія») і статтею 16(1) Договору про функціонування Європейського Союзу встановлено, що кожна особа має право на захист своїх персональних даних [9]. Європейська інституційна визначеність захисту даних стала прикладом для інших країн[1], що істотно вплинуло на підвищення вимог щодо захисту даних у багатьох юрисдикціях, водночас викликало негативну реакцію з боку глобальних інформаційних гігантів США [10], створивши довгострокову основу для геоекономічного інституційного протистояння США та ЄС у цій сфері.

Ефективність захисту даних в США значно нижча, ніж в ЄС, через поверховість і відсутність всеосяжності у законодавстві; норми права обмежені державним сектором, охороною здоров'я та банківською справою; підприємства інших сфер приватного сектора США розробляють та застосовують власні обмеження щодо захисту конфіденційності даних [10]. Загалом це відбувається для створення дружнього до інновації простору, при цьому регулювання захисту даних відбувається на ринкових засадах, що передбачають відносну самостійність ринкових суб'єктів щодо реалізації основних принципів захисту інформації. Водночас такі ліберальні підходи наражають ринкових суб'єктів на ризики витоку інформації, її небажаного розповсюдження та використання.

Прийняття в європейському інституційному просторі законодавчих актів, що стосувалися розвитку єдиного цифрового ринку, захисту даних, права на конфіденційність тощо наражалося на американську критику з боку як держави, так і ТНК через явні розбіжності у поглядах між ЄС та США щодо регулювання інформаційного та інноваційного середовища, доречності та адекватності державного втручання. Основна ідея, що була озвучена, – нове законодавство перешкоджатиме співпраці в галузі національної безпеки та вбиватиме інновації та дослідження [10].

Одним із перших законодавчих актів на рівні ЄС, прийнятих для формування єдиного цифрового ринку, був затверджений у 2016 році Загальний регламент про захист даних (GDPR, Регламент), який чітко визначає цілі, обсяги, механізми збору персональних даних і вимоги до державних та приватних установ, що збирають, систематизують та обробляють персональну інформацію: забезпечення її цілісності, безпеки і точності.

На сьогодні майже 120 країн ухвалили закони про конфіденційність на основі базових положень GDPR [10].

Наріжним каменем GDPR є встановлене статтею 17 «право бути забутим» (Article 17 GDPR. Right to erasure («right to be forgotten»)), застосування якого означає, що суб'єкт даних має право на видалення своїх персональних

[1] Глобальний вплив ЄС на процеси інституціоналізації в різних економічних сферах був названий Брюссельським ефектом. Див. Anu Bradford. The Brussels Effect: How the European Union Rules the World. https://books.google.com.ua/books?id=EU3 [10].

даних, яке повинен здійснити контролер без будь-якої безпідставної затримки, у разі виникнення однієї з визначених GDPR умов [11].

Основними підставами для видалення інформації про особу є:

- інформація більше не є потрібною в контексті первісних цілей її збору та систематизації;
- особа відкликає згоду на збір та обробку даних;
- збір, систематизація та використання персональних даних відбувається з метою прямого маркетингу, а фізична особа заперечує таку обробку;
- незаконне опрацювання персональних даних особи;
- видалення персональних даних для виконання юридичної ухвали або зобов'язання тощо.

Водночас Регламент також визначає право компанії, що обробляє дані, щодо її переваження над «правом особи бути забутою» у таких випадках:

- дані використовуються для здійснення права на свободу вираження поглядів та інформації;
- дані використовуються для виконання правової ухвали або зобов'язання;
- дані використовуються для виконання завдання, яке здійснюється у суспільних інтересах або під час здійснення офіційних повноважень організації;
- оброблювані дані необхідні для охорони здоров'я і слугують громадським інтересам;
- оброблювані дані необхідні у медичних цілях (у тому числі профілактичного характеру);
- дані являють собою важливу інформацію, яка служить суспільним інтересам, науковим дослідженням, історичним дослідженням або статистичним цілям, і видалення яких може утруднити або зупинити прогрес у досягненні мети, яка була метою обробки;
- дані використовуються для створення правового захисту або для здійснення інших правових вимог.

У такий спосіб було сформовано досить хитке підґрунтя для операційної активності користувача глобального інформаційного простору; адже широкий спектр випадків, коли організації можуть відхилити вимоги особи щодо видалення даних, зумовив другорядні позиції користувача по відношенню до глобальних інформаційних гігантів (ГІГ). Правозастосування із самого початку його реалізації стало обмежено ефективним, про що свідчить практика задоволення заявок клієнтів на видалення інформації.

Історичним прецедентом реалізації в ЄС права на видалення даних за вимогою особи було визнання судом права на забуття приватної особи (справа проти Google: C-131/12 – Google Spain v. Costeja González (2014)) [12]. Водночас ця справа не стала основою для встановлення автоматичного обов'язку видаляти будь-які згадки, а лише ті, які є неактуальними, недоречними, надмірними чи неточними.

Тим паче, справа 2019 року, що виникла в результаті звернення Google до Державної ради Франції (Conseil d'État) із запитом щодо скасування рішення французького наглядового органу CNIL щодо накладення штрафу у розмірі 100 тис. євро, визначила географічні умови правозастосування. Штраф був накладний «у зв'язку з невиконанням вимог офіційного сповіщення, згідно з яким компанія Google була зобов'язана при задоволенні запиту від осіб щодо видалення посилань на веб сторінки з переліку результатів пошуку за їхніми іменами застосувати таке видалення до всіх розширень доменних імен своєї пошукової системи» [13]. «Суд ЄС зауважив, що законодавство ЄС не вимагало від оператора пошукової системи видаляти посилання в усіх версіях його пошукової системи. Однак він був зобов'язаний їх видалити у версіях пошукової системи в усіх Державах-членах і вжити заходів, що перешкоджали б доступу інтернет-користувачів, які здійснюють пошук в одній з держав-членів, до відповідних посилань, у версіях пошукової системи, розташованих за межами ЄС» [13].

Подальші справи проти Google показали явну домінанту глобального інформаційного гіганта над користувачами. Так, справа проти Google 2022 року [14] полягала в оскарженні відмови компанії видалити посилання, що містили недостовірну інформацію. При цьому суд ЄС уточнив зобов'язання особи щодо доказу явної неправдивості інформації і додав, що «від оператора пошукової системи не можна було вимагати активної ролі у намаганні встановити факти, щодо яких не було наведено доказів у запиті про видалення посилань, з метою визначити, чи був запит обґрунтованим. Таке зобов'язання накладало б на цього оператора надмірний тягар і створило б серйозний ризик того, що контент, який задовольняє потребу громадськості в інформації, квазісистематично вилучався б з індексації оператором для уникнення тягаря розслідування» [14].

Рішення суду показало істотні викривлення у правозастосуванні, що на поверхні взаємодії користувачів з глобальними інформаційними гігантами проявляється у невтішних тенденціях:

- непогодження осіб на наявність даних у вільному доступі не є достатньою підставою для видалення;
- особа має надавати докази про неправдивість інформації;
- пошукова система має право на відмову у видаленні інформації;
- пошукова система не бере участі у доведенні істинності інформації, незважаючи на наявність прецеденту розповсюдження нею неправдивої інформації;
- пошукова система не має наражатися на ризики можливих розслідувань;
- якщо не було звернення в суд щодо її діяльності, пошукова система лишається абсолютним інформаційним монополістом щодо володіння та використання інформації.

Позасудова практика реалізації права осіб на забуття доводить попередні тези щодо особливостей взаємодії корпорацій та користувачів. Звіти Google Transparency Report демонструють, що відхилення запитів на видалення інформації є укоріненою тенденцією. Згідно з рішенням Суду Європейського Союзу від травня 2014 року, вказаним вище, користувачі мають право надсилати в пошукові системи запити на видалення результатів пошуку, які містять інформацію про них. Водночас з травня 2014 по квітень 2025 року з боку Google було задоволено лише 51,5% відповідних запитів користувачів, 48,5 % запитів було відхилено через суспільний інтерес [15].

Поняття *суспільного інтересу* використовується в багатьох законодавчо-нормативних документах ЄС і охоплює широке коло питань, які мають значення для громадськості. Як зазначає Маріц Д., Європейський суд з прав людини виробив ряд фундаментальних принципів, що стосуються діяльності журналістів в аспекті поширення інформації, «що становить суспільний інтерес: 1) належне повідомлення інформації та ідей стосовно питань, які становлять громадський інтерес; 2) належне повідомлення про роботу судів; 3) ведення політичної дискусії; 4) твердження про брутальність; 5) представлення в репортажі соціальної проблеми; 6) захист та компенсація за шкоду, завдану в результаті наукових розробок тощо» [16]. У Пропозиції щодо Директиви Європейського Парламенту та Ради про захист осіб, які беруть участь у громадському житті, поняття суспільного інтересу означає будь-яке питання, «яке впливає на громадськість настільки, що вона може законно цікавитися ним, у таких сферах, як: громадське здоров'я, безпека, навколишнє середовище, клімат, здійснення основних прав» [17].

Визначення суспільного інтересу самою корпорацією Google виглядає надто нечітко та розмито. На сторінці Google Transparency Report вказано, що «визначення суспільного інтересу – складний процес, під час якого потрібно враховувати різноманітні фактори, зокрема такі: чи стосується вміст професійної діяльності автора запиту, минулого злочину, політичної посади, участі в суспільному житті, а також, чи такий вміст, створений автором, є документом державного зразка чи публіцистичним матеріалом» [18]. Практика правозастосування показує відсутність прозорих критеріїв "суспільного інтересу", що залишає користувача в зоні тотального панування інформаційного гіганта.

Головною проблемою реалізації «права бути забутим» є тривалий та глибоко укорінений диспаритет у взаємовідносинах між інформаційними гігантами та користувачами. Домінантне положення Big Tech закріплюється через те, що переважна більшість запитів на видалення інформації – 90,7%, – поступає від найбільш вразливої та незахищеної категорії користувачів – приватних осіб [15], а результати звернення про видалення знаходяться у площині доброї волі контролера (пошукової системи, ЗМІ тощо).

На цьому тлі амбівалентно виглядає статистика задоволення глобальних запитів щодо особистих даних користувачів, наданих Google на вимогу державних органів. Це свідчить про більш пильну увагу Google до питань глобальної безпеки та взаємодії на цій основі з державними та наднаціональними регуляторами, ніж до захисту прав користувачів. Той же Google Transparency Report свідчить про 80-відсоткове задоволення запитів державних органів на доступ до даних користувачів для розслідування цивільних, адміністративних і кримінальних справ, а також загроз національній безпеці [19].

Вже сьогодні очевидно, що правозастосування норми «права бути забутим» в ЄС має системні викривлення, реалізується фрагментарно, залежно від юрисдикції та сили особи (приватна особа проти корпорації); розгляд запиту, якщо не було звернення в суд, залишається на розсуд корпорації (Google, Meta); прецеденти судових справ з Google доводять, що домінуючою стороною при вирішення спорів є корпорація, а не приватна особа. Все це показує обмежено дієвий характер інституціоналізації захисту інформації в європейській правовій системі координат в частині реалізації «права на забуття».

Більш ефективний нагляд сьогодні забезпечений для реалізації положення Регламенту «Конфіденційність як першочерговість», за неналежне виконання якого компанії підлягають штрафу у розмірі до 20 мільйонів євро або до 4 % від загального світового доходу компанії за попередній фінансовий рік.

Статистика розгляду порушень показує зростання компетентності органів захисту даних у Європі як на наднаціональному рівні, так і на рівні національних держав. Нагляд за правозастосуванням та статистика штрафів свідчить про ідентичність підходів як до компаній національного рівня, так і транснаціональних корпорацій. У 2023 році Ірландія наклала рекордний штраф на Facebook – 1,2 млрд євро, усього ж за порушення GDPR підприємства та державні установи були оштрафовані на 4,4 мільярди євро [20].

Штрафні санкції використовуються європейськими органами нагляду за захистом даних для спонукання компаній *щодо зміни бізнес-моделей* відповідно до законодавства.

Найбільші штрафи, накладені європейськими органами нагляду, наведені у табл. 1.

Досвід використання основних положень GDPR до глобальних інформаційних гігантів демонструє спроби наглядових органів європейських країн щодо забезпечення діяльності глобальних корпорацій відповідно до вимог ЄС. У перспективі очікується глобальна уніфікація підходів комплаєнсу в частині захисту даних через явну складність та економічну неефективність адаптації практики ведення бізнесу до різних юрисдикцій [10]. Вважається, що врахування економічних ефектів операційної активності, зумовлених значними обсягами європейського ринку, має стимулювати глобальних гравців до відповідності європейському законодавству. Facebook має понад 250 мільйонів користувачів у Європі, що забезпечують 25 % світового прибутку Facebook. У більшості країн – членів ЄС частка Google на ринку пошуку становить понад 90 %, що перевищує 67–75 % ринку у Сполучених Штатах [10]. Але це формальна сторона питання.

Реалії ж такі, що все більш очевидними стають тенденції обмеженого європейського втручання в певні сфери діяльності глобальних інформаційних гігантів (нагляд за «правом бути забутим») та втручання постфактум в умовах відсутності дійових превентивних заходів (захист права на конфіденційність). GDPR дійсно є найсуворішим законодавством щодо захисту персональних даних у світі, але механізми впливу на Big Tech неоптимальні з точки зори соціальних стандартів або запізнілі, вони не стимулюють зміни у бізнес-моделі, побудованої на автоматичному зборі інформації про користувачів, не змінюють механізмів персоналізації пошуку або непрозорість алгоритмів.

Відчувається явна нерішучість європейських наднаціональних органів нагляду стосовно Big Tech. Незважаючи на зростаючі обсяги накладених штрафів, ефекти діяльності регуляторів не відповідають повною мірою заявленим цілям захисту даних. Загалом же, як показує практика, су-

Таблиця 1

Ефективність нагляду на основі GDPR

Рік	Компанія	Сутність справи	Сума штрафу
2019	British Airways	Халатність щодо захисту даних клієнтів, що призвело до зламу даних 400 000 осіб (імена, адреси, номери CVV їхніх кредитних карток)	€183 млн, але в 2020 році ця сума була зменшена до €20 млн через COVID-19
2020	H&M	Порушення безпеки даних співробітників шляхом запису розмов співробітників і зберігання відповідного матеріалу у вільному доступі без їх попереднього повідомлення	€35,3 млн
2019	Google	Неналежне повідомлення клієнтів про збір і обробку їхніх даних для здійснення адресної реклами	€ 50 млн
2021	Amazon	Обробка даних клієнтів для цільової реклами без їх згоди. Це не перший випадок відповідних звинувачень, вперше це відбулося у 2020 році	€ 746 млн
2022	Google	Штраф з боку французьких регуляторів безпеки даних за порушення політики щодо файлів cookie	€ 150 млн
2022	Facebook (Meta)	Штраф з боку ірландських регуляторів безпеки даних за нездатність вжити належних технологічних та організаційних заходів для захисту конфіденційності даних своїх користувачів. 12 порушень захисту даних за 6 місяців	€ 17 млн
2023	Facebook	Найбільший штраф в історії GDPR наклав ірландський орган захисту даних спільно з Радою захисту даних Європейського Союзу за те, що платформа відправляє дані користувачів Facebook з країн Європейського Союзу до США	€ 1,2 млрд

Джерело: систематизовано за даними: [21; 22; 23; 24; 25; 26]

дові справи проти глобальних корпорацій можуть тривати роками [27].

Проблема захисту даних в ЄС розгортається через очевидне домінування глобальних інформаційних гігантів неєвропейського походження у сфері постачання технологічної продукції. Так, згідно зі звітом Маріо Драгі про конкурентоспроможність Європи від вересня 2024 року, понад 80% цифрових технологій та інфраструктури в Європі імпортуються. Залежність стосується, перш за все, США та Китаю, а також кількох технологічних компаній з цих країн [28]. Згідно з дослідженнями Synergy Group [29], американські постачальники, такі як Amazon, Microsoft та Google, домінують майже на 70% європейського ринку хмарних обчислень. Найбільший європейський постачальник має лише 2% частки ринку. Крім того, близько 70% базових моделей штучного інтелекту (ШІ), що використовуються в усьому світі, походять зі США.

Зовнішня інноваційна залежність Європи обмежує політичну волю втручання регуляторів для уникнення ризиків цифрового паралічу. Тому контроль за виконанням норм GDPR приймає форму балансування між довгостроковими цілями усталеного інноваційного руху і актуальними цілями забезпечення виконання норм захисту даних.

З одного боку, держави намагаються все міцніше ставати на стражі національних пріоритетів захисту інформації, з другого боку – глобальні інформаційні гіганти продовжують діяльність поза принципами комплаєнсу у сфері захисту даних, наочним є загострення конфлікту інтересів.

У цьому русі деякі країни проявляють найбільшу міць, самостійність і рішучість. Ірландія, Франція, Люксембург є країнами, де наглядові органи найбільш активні щодо правозастосування норм GDPR щодо до глобальних корпорацій [30] .

Загалом же, згідно з даними звіту GDPR Enforcement Tracker Report, станом на 1 березня 2024 року загальна кількість штрафів, накладених національними органами контролю за захистом даних європейських країн, досягла 2086 (+510 у порівнянні зі звітом GDPR Enforcement Tracker Report 2023). Загальна сума накладених штрафів – близько 4,48 мільярда євро (+1,71 мільярда порівняно зі звітом GDPR Enforcement Tracker Report 2023) [30].

Дані показують, що на сьогодні найвищі штрафи стягувалися в секторах «ЗМІ, телекомунікації та телерадіомовлення», «Промисловість і торгівля», «Транспорт і енергетика». Крім того, секторами з найвищою кількістю штрафів є: «ЗМІ, телекомунікації та радіомовлення» та «Промисловість і торгівля». Як свідчать європейські експерти, така ситуація пов'язана не тільки з тим, що у цих секторах підприємства схильні нехтувати вимогами GDPR, а й з тим, що у секторах велика кількість компаній, або було накладено великі суми штрафів у розрахунку на одну компанію. Крім того, у такій країні, як Іспанія, спостерігається підвищена увага та зосередженість влади на секторі ЗМІ, телекомунікацій і телерадіомовлення, де іспанська влада вже виписала понад 60 штрафів проти конкретного іспанського постачальника телекомунікацій. Порівняно мало штрафів у сферах «Проживання та готельний бізнес» і «Не-

рухомість». Поки це також стосується сектора «Транспорт та енергетика», штрафи в цьому секторі мали високий середній показник суми [30].

Країнами з найактивнішими наглядовими органами щодо виконання вимог GDPR у частині накладення штрафів були Іспанія, Італія, Румунія, Німеччина, Угорщина, Польща, Греція. Найбільшу активність проявив іспанський орган із захисту даних із *загальною кількістю* 802 штрафи (+219 порівняно з GDPR Enforcement Tracker, Звіт 2022). Іншими країнами з порівняно високою активністю є Італія, Румунія та Німеччина, які наклали від 74 до 343 (опублікованих) штрафів. Проте ці три країни разом мають менше штрафів, ніж в Іспанії [30].

Якщо дивитися на *загальну суму* штрафів, стягнену у країнах, то лідирує Ірландія, потім Люксембург, Франція, Італія, Іспанія [30].

Основними видами правопорушень були:

- недостатня правова база для обробки даних;
- недостатні технічні та організаційні заходи щодо забезпечення інформаційної безпеки;
- недотримання загальних принципів обробки даних;
- недостатнє дотримання прав суб'єктів даних;
- недостатнє виконання зобов'язань щодо інформації;
- недостатня співпраця з наглядовим органом;
- недостатнє виконання зобов'язань щодо повідомлення про порушення даних;
- відсутність призначення уповноваженого із захисту даних [30].

На сьогодні ми все частіше спостерігаємо конфліктні форми взаємодії держави та транснаціональних корпорацій, що є інформаційними гігантами. Їхнім головним ризиком стає можливість практично миттєвої зміни розстановки політичних та економічних сил на глобальній арені, зважаючи на обсяги конфіденційної інформації, що є у розпорядженні ГІГ, та ризики інформаційних витоків. Все це створюватиме умови перманентної невизначеності, яку долатимуть посиленням адміністративних методів, включаючи вплив правоохоронних органів, що, зокрема, показало протистояння між мережею Telegram та французькою владою.

Незважаючи на активність наглядових органів певних країн щодо захисту даних, в ЄС існує проблема фрагментарності у використанні європейського законодавства та відсутності єдиних європейських наглядових підходів [31].

На цьому тлі поступово змінюються риторика наднаціональних наглядових органів в ЄС від більш консервативних поглядів до лібералізації процесів інституціоналізації, що проявляється у спрощенні нагляду під знаком сприяння бізнесу [32], але на практиці це може означати неусталеність законодавчих підходів, створюватиме ризики невизначеності правового поля.

Сьогодні можна спостерігати, як трансформується регуляторна логіка в ЄС в бік зменшення адміністративного тиску та розповсюдження пом'якшувальних заходів у процесі застосування норм GDPR малими та середніми підприємствами і малими підприємствами середньої капіталізації. Ці заходи надають більшу самостійність підприємствам у виборі методів забезпечення відповідності їх операційної активності нормам GDPR. Водночас це тільки початок, і в інноваційних перегонах ніхто не застрахований від подальшої лібералізації європейського законодавства у сфері захисту даних, особливо коли наріжним стає питання конкурентної боротьби в глобальному інноваційному просторі та економічної безпеки.

Законодавчі нововведення свідчать про прагнення ЄС знайти баланс між захистом прав громадян та стимулюванням інновацій. Проте деякі експерти висловлюють занепокоєння, що спрощення нагляду може призвести до недостатнього захисту персональних даних і прав користувачів.

Поступовий зсув у сфері європейської інституціоналізації цифрового переходу від домінування прав людини до переваги економічної безпеки триває як результат не тільки внутрішнього бізнес-стимулювання, але як результат прогресуючого зростання влади глобальних цифрових гігантів і глобально-монополістичної інформаційної асиметрії, – вкоріненого інформаційного домінування корпорацій над їх користувачами внаслідок використання переваг володіння передовими технологіями збору, систематизації інформації в економічних та соціогуманітарних цілях корпорацій [33].

У такому русі важливо усвідомлювати, що захист користувача має бути на першому місці при прийнятті відповідних рішень, адже завжди існує істотний дисбаланс у використанні інформації, зумовлений інформаційною асиметрією. У цифровому суспільстві він приймає особливу форму. Зростаючі обсяги даних в інформаційному просторі стають інформаційним профіцитом для пересічного користувача і значно утруднюють процеси прийняття рішень в умовах збільшення невизначеності. Водночас для інформаційного гіганта вся інформація може бути відповідним чином систематизована і використана, не сьогодні, так у майбутньому; для нього це умови інформаційної достатності.

У цьому прослідкується важлива суперечність – спроби інституціоналізувати захист даних для забезпечення впорядкування глобального інформаційного простору насправді результатом мають зростаючі ризики невизначеності для обивателя інформаційного простору.

Висновки.

1. Глобальна проблема захисту даних має виражений геоекономічний контекст, демонструючи суперечності між глобальними інформаційними гігантами (Google, Facebook тощо), що керуються міркуваннями технологічного просування та економічної вигоди, та європейськими країнами, що визнають та інституціоналізують право на захист інформації як наріжне суб'єктне право.
2. У ЄС впроваджено найміцніше у світі законодавство у сфері захисту даних (зокрема, Загальний регламент про захист даних), водночас досвід правозастосування його основних положень висвітлює обмежену інституційну ефективність європейського правового поля внаслідок технологічної залежності від компаній неєвропейського

походження. Правозастосування окремих норм щодо захисту даних в ЄС (наприклад, «права бути забутим») реалізується фрагментарно з явною правовою перевагою на боці глобальних інформаційних гігантів, що виражається не у прямій підтримці з боку регуляторної спільноти ЄС, а у практиці обмеженого втручання. Це доводить суперечливий характер інституціоналізації захисту даних в ЄС.

3. Як результат технологічного тиску з боку глобальних корпорацій в ЄС поступово змінюються підходи наглядових органів від більш консервативних до лібералізаційних. Незважаючи на формальну аргументацію цих процесів в руслі сприяння бізнесу та інноваціям, фактично це може означати рухливість законодавчих принципів у первісно міцному законодавстві та призвести до недостатнього захисту персональних даних та прав користувачів.
4. Національні наглядові органи у сфері захисту даних країн ЄС демонструють більшу виваженість, послідовність і твердість у сфері захисту даних, ніж наднаціональні; про це свідчить досвід судових справ, штрафів, накладених на, у тому числі, глобальні корпорації; що доводить їх принципову позицію поза залежності від юрисдикції порушників європейського законодавства.
5. Досвід європейського правозастосування норм законодавства у сфері захисту даних підтверджує давню європейську тенденцію певного інституційного індивідуалізму залежно від завдань національної політики країн-учасниць, внутрішньої інституційної рішучості та сили впливу неформальних інститутів; і саме ці фактори відіграють головну роль у процесі правозастосування, а не єдність цифрового простору та його унормування.
6. Зважаючи на низький рівень кібербезпеки в Україні та часті інформаційні витоки, Україні потрібна імплементація європейських норм захисту даних як в частині застосування Загального регламенту про захист даних, так і в частині створення відповідного наглядового органу; зважаючи на те, що вже більше 120 країн світу у процесі інституціоналізації захисту даних прийняли за основу саме цей Регламент.
7. Водночас вже сьогодні зрозуміло, що імплементація європейського законодавства та створення наглядових структур не означитиме автоматичної відповідності українського інституційного середовища європейським стандартам. Потрібна правова воля і рішучість держави діяти у контексті захисту прав найуразливішої частини суб'єктів інформаційного простору – користувачів.
8. Необхідним і достатнім елементом інституціоналізації захисту даних в Україні є створення платформи (за прикладом ЄС, де існує GDPR Enforcement Tracker), що представляє статистику правопорушень та відповідних накладених штрафів за порушення компаніями норм захисту даних; це формуватиме відкритий прозорий простір відповідального відношення та транспарентного клімату у сфері захисту даних.
9. Для уникнення можливих штрафних витрат та недопущення шкоди репутації українським компаніям вже сьогодні потрібно інвестувати у забезпечення дотримання правил захисту даних, починаючи із структурованого огляду того, чому та які персональні дані обробляються.
10. Водночас слід брати до уваги, що європейський досвід захисту даних демонструє явне домінування глобальних інформаційних корпорацій, їх небажання змінювати алгоритми збору, обробки та використання інформації, їх переважне положення в правовому полі, що ще раз підкреслює існування глобально-монополістичної інформаційної асиметрії, яка стає природним явищем цифрового суспільства, проти якої немає дійової системи захисту, незважаючи на досвід міцної інституціоналізації.

ЛІТЕРАТУРА

1. Економічні переваги від інтеграції в Єдиний цифровий ринок ЄС: названі реальні цифри // Міністерство цифрової трансформації. 15 грудня 2020 р. URL: https://thedigital.gov.ua/news/ekonomichni-perevagi-vid-integratsii-v-ediniy-tsifroviy-rinok-es-nazvani-realni-tsifri

2. Digital single market for Europe. The European Council, The Council of the European Union. 21.09.2020. URL: https://www.consilium.europa.eu/en/policies/digital-single-market/

3. Гриценко А., Песоцька Є. Формування інформаційно-мережевої економіки. *Економічна теорія.* 2013. № 1. С. 5–19.

4. Биков О. М., Савченко В. В. Захист персональних даних у сучасному законодавстві. *Legal Bulletin*. 2024. № 14. С. 67–72. DOI: https://doi.org/10.31732/2708-339X-2024-14-A9

5. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти. Страсбург : Рада Європи, 2021. 157 с.

6. Пилипчук В. Г., Брижко В. М. Реформування і розвиток системи захисту персональних даних в Україні. *Інформація і право*. 2022. № 3. С. 5–21.

7. Baghal-Schmid A., Esser L. Numbers and Figures. 2024. URL: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures

8. Jahangir R. The GDPR Shake-Up: What You Need to Know // *TechPolicy.Press.* 2025. URL: https://www.techpolicy.press/the-gdpr-shakeup-what-you-need-to-know/

9. Регламент (ЄС) 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, яким скасовується Директива 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

10. Bradford A. The Brussels Effect: How the European Union Rules the World. URL: https://books.google.com.ua/books?id=EU3-xwEACAAJ&pg=PR7&hl=ru&source=gbs_selected_pages&cad=2#v=onepage&q&f=false

11. Article 17 GDPR. Right to erasure ('right to be forgotten'). URL: https://gdpr-text.com/uk/read/article-17/

12. Global freedom of Expression. URL: https://global freedomofexpression.columbia.edu/wp-content/uploads/2021/12/Googlev.AgenciaEsp_Russian.pdf

13. Рішення Суду ЄС від 24 вересня 2019 року у справі «Гугл» (Google), C-507/17, EU:C:2019:772. URL: https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten-ukr

14. Рішення Суду ЄС від 08 грудня 2022 року у справі «Гугл» (Google) (Видалення посилань на стверджувану неправдиву інформацію), C-460/20, EU:C:2022:962. URL: https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten-ukr

15. Запити на видалення контенту відповідно до законодавства ЄС у сфері захисту персональних даних – Звіт Google про доступність сервісів і даних. URL: https://transparencyreport.google.com/eu-privacy/overview?hl=uk

16. Маріц Д. Поняття «суспільний інтерес» у інформаційних правовідносинах. *Інформаційне право*. 2018. № 11. С. 167.

17. Proposal for a Directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings ("Strategic lawsuits against public participation"). 27.04.2022. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0177

18. Довідковий центр Звіту про доступність сервісів і даних // Суспільний інтерес. URL: https://support.google.com/transparencyreport/answer/7347822?hl=uk

19. Глобальні запити щодо особистих даних користувачів. Звіт про доступність сервісів і даних. URL: https://transparencyreport.google.com/user-data/overview?hl=uk&user_data_produced=authority:;series:compliance&lu=user_data_produced

20. New record for GDPR fines: over four billion euros in penalties. URL: https://www.gdprregister.eu/news/new-record-for-gdpr-fines-over-four-billion-euros-in-penalties/

21. ICO fines British Airways £20m for data breach affecting more than 400,000 customers. URL: https://www.gdprregister.eu/news/british-airways-fine

22. H&M gets 35.3M euros fine for records of private living conditions of employees. URL: https://www.gdprregister.eu/news/hm-gdpr-fine

23. Google: US Tech Giant and the Record-High Fine Under the GDPR. URL: https://www.gdprregister.eu/news/google-biggest-fine

24. Amazon considers appeal after court sides with regulator on record privacy fine. URL: https://www.euronews.com/next/2025/03/20/amazon-considers-appeal-after-court-sides-with-regulator-on-record-privacy-fine

25. 1.2 billion euro fine for Facebook as a result of EDPB binding decision. URL: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

26. New record for GDPR fines: over four billion euros in penalties. URL: https://www.gdprregister.eu/news/new-record-for-gdpr-fines-over-four-billion-euros-in-penalties/

27. Google and Apple Face Billions in Penalties After Losing E.U. Appeals. URL: https://www.nytimes.com/2024/09/10/technology/european-union-apple-google-antitrust.html

28. The future of European competitiveness: Report by Mario Draghi. URL: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

29. Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs. URL: https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs

30. Schmid A. Numbers and Figures What has happened so far, expressed in numbers. URL: https://cdn.lawreportgroup.com/acuris/files/Cybersecurity-

31. Germany says GDPR could collapse as Ireland dallies on big fines. URL: https://www.wired.com/story/gdpr-fines-google-facebook/

32. Євросоюз має плани спростити закон GDPR про конфіденційність персональних даних, бо він заважає бізнесу // Судово-юридична газета. URL: https://sud.ua/uk/news/publication/327449-evrosoyuz-planiruet-uprostit-zakon-gdpr-o-konfidentsialnosti-personalnykh-dannykh-poskolku-on-meshaet-biznesu

33. Корнівська В. Інститути фінансового посередництва в процесі формування інформаційно-мережевої економіки. Київ : ІЕПр НАН України, 2018. 436 с.

REFERENCES

2 billion euro fine for Facebook as a result of EDPB binding decision. URL: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Amazon considers appeal after court sides with regulator on record privacy fine. URL: https://www.euronews.com/next/2025/03/20/amazon-considers-appeal-after-court-sides-with-regulator-on-record-privacy-fine

Article 17 GDPR. Right to erasure ('right to be forgotten'). URL: https://gdpr-text.com/uk/read/article-17/

Baghal-Schmid, A., & Esser, L. (2024). Numbers and Figures. URL: https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report/numbers-and-figures

Bem, M., & Horodyskyi, I. (2021). *Zakhyst personalnykh danykh: pravove rehuliuvannia ta praktychni aspekty* [Protection of personal data: Legal regulation and practical aspects]. Rada Yevropy.

Bradford, A. The Brussels Effect: How the European Union Rules the World. URL: https://books.google.com.ua/books?id=EU3-xwEACAAJ&pg=PR7&hl=ru&source=gbs_selected_pages&cad=2#v=onepage&q&f=false

Bykov, O. M., & Savchenko, V. V. (2024). *Zakhyst personalnykh danykh u suchasnomu zakonodavstvi* [Protection of personal data in modern legislation]. *Legal Bulletin*, *14*, 67–72. https://doi.org/10.31732/2708-339X-2024-14-A9

Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs. URL: https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs

Dovidkovyi tsentr Zvitu pro dostupnist servisiv i danykh // Suspilnyi interes. URL: https://support.google.com/transparencyreport/answer/7347822?hl=uk

The European Council, The Council of the European Union. (2020, 21 veresnia). Digital single market for Europe. URL: https://www.consilium.europa.eu/en/policies/digital-single-market/

Germany says GDPR could collapse as Ireland dallies on big fines. URL: https://www.wired.com/story/gdpr-fines-google-facebook/

Global freedom of Expression. URL: https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/12/Googlev.AgenciaEsp_Russian.pdf

Google: US Tech Giant and the Record-High Fine Under the GDPR. URL: https://www.gdprregister.eu/news/google-biggest-fine

Google and Apple Face Billions in Penalties After Losing E.U. Appeals. URL: https://www.nytimes.com/2024/09/10/technology/european-union-apple-google-antitrust.html

H&M gets 35.3M euros fine for records of private living conditions of employees. URL: https://www.gdprregister.eu/news/hm-gdpr-fine

Hlobalni zapyty shchodo osobystykh danykh korystuvachiv. Zvit pro dostupnist servisiv i danykh. URL: https://transparencyreport.google.com/user-data/overview?hl=uk&user_data_produced=authority:;series:compliance&lu=user_data_produced

Hrytsenko, A., & Pesotska, Ye. (2013). *Formuvannia informatsiino-merezhevoi ekonomiky* [Formation of information network economy]. *Ekonomichna teoriia*, *1*, 5–19.

ICO fines British Airways £20m for data breach affecting more than 400,000 customers. URL: https://www.gdprregister.eu/news/british-airways-fine

Jahangir, R. (2025). The GDPR Shake-Up: What You Need to Know. *TechPolicy.Press*. URL: https://www.techpolicy.press/the-gdpr-shakeup-what-you-need-to-know/

Kornivska, V. (2018). *Instytuty finansovoho poserednytstva v protsesi formuvannia informatsiino-merezhevoi ekonomiky* [Institutions of financial intermediation in the formation of the information network economy]. IEPr NAN Ukrainy.

Marits, D. (2018). *Poniattia «suspilnyi interes» u informatsiinykh pravovidnosynakh* [The concept of "public interest" in information legal relations]. *Informatsiine pravo*, *11*, 167.

Ministerstvo tsyfrovoi transformatsii. (2020, 15 hrudnia). *Ekonomichni perevahy vid intehratsii v Yedynyi tsyfrovyi rynok YeS: nazvani realni tsyfry* [Economic benefits from integration into the EU Digital Single Market: Real figures named]. URL: https://thedigital.gov.ua/news/ekonomichni-perevagi-vid-integratsii-v-ediniy-tsifroviy-rinok-es-nazvani-realni-tsifri

New record for GDPR fines: over four billion euros in penalties. URL: https://www.gdprregister.eu/news/new-record-for-gdpr-fines-over-four-billion-euros-in-penalties/

New record for GDPR fines: over four billion euros in penalties. URL: https://www.gdprregister.eu/news/new-record-for-gdpr-fines-over-four-billion-euros-in-penalties/

Proposal for a Directive of the European Parliament and of the Council on protecting persons who engage in public participation from manifestly unfounded or abusive court proceedings ("Strategic lawsuits against public participation"). (2022, 27 kvitnia). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0177

Pylypchuk, V. H., & Bryzhko, V. M. (2022). *Reformuvannia i rozvytok systemy zakhystu personalnykh danykh v Ukraini* [Reforming and developing the system of personal data protection in Ukraine]. *Informatsiia i pravo*, *3*, 5–21.

Rehlament (YeS) 2016/679 Yevropeiskoho parlamentu i Rady vid 27 kvitnia 2016 roku pro zakhyst fizychnykh osib u zv'yazku z opratsiuvanniam personalnykh danykh i pro vilnyi rukh takykh danykh, yakym skasovuietsia Dyrektyva 95/46/YeS (Zahalnyi rehlament pro zakhyst danykh). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

Rishennia Sudu YeS vid 08 hrudnia 2022 roku u spravi «Huhl» (Google) (Vydalennia posylan na stverdzhuvanu nepravdyvu informatsiiu), C-460/20, EU:C:2022:962. URL: https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten-ukr

Rishennia Sudu YeS vid 24 veresnia 2019 roku u spravi «Huhl» (Google), C-507/17, EU:C:2019:772. URL: https://ks.echr.coe.int/documents/d/echr-ks/right-to-be-forgotten-ukr

Schmid, A. Numbers and Figures What has happened so far, expressed in numbers. URL: https://cdn.lawreportgroup.com/acuris/files/Cybersecurity-Germany

Sudovo-yurydychna hazeta. (n.d.). Yevrosoiuz maie plany sprostyty zakon GDPR pro konfidentsiinist personalnykh danykh, bo vin zavazhaie biznesu [The European Union plans to simplify the GDPR law on personal data privacy, as it interferes with business]. URL: https://sud.ua/uk/news/publication/327449-evrosoyuz-planiruet-uprostit-zakon-gdpr-o-konfidentsialnosti-personalnykh-dannykh-poskolku-on-meshaet-biznesu

Zapyty na vydalennia kontentu vidpovidno do zakonodavstva YeS u sferi zakhystu personalnykh danykh – Zvit Google pro dostupnist servisiv i danykh. URL: https://transparencyreport.google.com/eu-privacy/overview?hl=uk

The future of European competitiveness: Report by Mario Draghi. URL: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en

Стаття надійшла до редакції 25.08.2025 р.

Статтю прийнято до публікації 10.09.2025 р.