УДК 341.2
DOI https://doi.org/10.32782/2663-6170/2025.43.30

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ІНТЕРНЕТ-ПРОСТОРІ ТА ЗАСАДИ КОНТРОЛЮ МЕХАНІЗМІВ СТЕЖЕННЯ ЗА КОРИСТУВАЧАМИ ЦИФРОВИХ ПЛАТФОРМ У ДЕРЖАВАХ ЄС

PROTECTION OF PERSONAL DATA IN THE INTERNET AND PRINCIPLES OF CONTROL OF MECHANISMS FOR MONITORING USERS OF DIGITAL PLATFORMS IN EU COUNTRIES

Сидор А.В.,
orcid.org/0009-0008-3776-991X
аспірант кафедри міжнародних відносин і дипломатичної служби
Львівського національного університету імені Івана Франка

У статті надається всебічний аналіз правових та інституційних механізмів Європейського Союзу щодо захисту свободи Інтернету як інтегрованого комплексу основних прав – права на приватність, свободи вираження поглядів, доступу до інформації та цифрової рівності. У ній концептуалізується режим цифрових прав ЄС як форма цифрового конституціоналізму, в якому наднаціональне законодавство, судове тлумачення та адміністративне виконання взаємодіють у рамках багаторівневої системи управління. Головною аналітичною проблемою, порушеною в дослідженні, є розрив між нормативною повнотою архітектури цифрових прав ЄС та її нерівномірним впровадженням у державах-членах. Ця розбіжність виникає через відмінності в адміністративному потенціалі, політичній волі та технологічній розвиненості, що разом створюють фрагментовану та асиметричну сферу захисту прав. Методологічно в дослідженні використовується порівняльний правовий, інституційний та системний аналіз для вивчення того, як Загальний регламент про захист даних (GDPR), Закон про цифрові послуги та пов'язані з ними регуляторні інструменти функціонують у рамках національних та наднаціональних структур, що перетинаються. Дослідження показує, що, хоча законодавча модель ЄС є глобально впливовим стандартом управління, заснованим на правах людини, її виконання обмежується процедурними перешкодами, плюралізмом юрисдикцій та зростаючою владою приватних цифрових посередників. Особлива увага приділяється ролі органів захисту даних, координаторів цифрових послуг та судів у формуванні операційної узгодженості регуляторного режиму. У статті стверджується, що нинішня система ЄС відображає складний баланс між захистом прав людини та технологічними інноваціями, проте вона залишається вразливою до непослідовності та регуляторної втоми. Розглядаючи ЄС як лабораторію цифрового конституціоналізму, дослідження підкреслює як трансформаційний потенціал, так і структурні обмеження наднаціонального управління в забезпеченні ефективної реалізації прав людини в цифровому середовищі.

Ключові слова: інтернет-свобода, Європейський Союз, цифровий конституціоналізм, захист даних, багаторівневе управління, алгоритмічна підзвітність, права людини в Інтернеті.

The article provides a comprehensive analysis of the European Union's legal and institutional mechanisms for protecting Internet freedom as an integrated set of fundamental rights – the right to privacy, freedom of expression, access to information, and digital equality. It conceptualises the EU's digital rights regime as a form of digital constitutionalism, in which supranational legislation, judicial interpretation and administrative enforcement interact within a multi-level governance system. The main analytical problem identified in the study is the persistent gap between the normative completeness of the EU's digital rights architecture and its uneven practical implementation in member states. This discrepancy arises from differences in administrative capacity, political will, and technological sophistication, which together create a fragmented and asymmetrical sphere of rights protection. Methodologically, the study uses comparative legal, institutional, and systemic analysis to examine how the GDPR, the Digital Services Act, and related regulatory instruments function within overlapping national and supranational structures. The study shows that although the EU legislative model is a globally influential human rights-based governance standard, its implementation is limited by procedural barriers, jurisdictional pluralism, and the growing power of private digital intermediaries. Particular attention is paid to the role of data protection authorities, digital service coordinators, and courts in shaping the operational coherence of the regulatory regime. The article argues that the current EU system reflects a complex balance between human rights protection and technological innovation but remains vulnerable to inconsistency and regulatory fatigue. Viewing the EU as a laboratory for digital constitutionalism, the study highlights both the transformative potential and the structural limitations of supranational governance in ensuring the effective realization of human rights in the digital environment.

Key words: Internet freedom, European Union, digital constitutionalism, data protection, multilevel governance, algorithmic accountability, human rights on the Internet.

Постановка проблеми. Цифрова трансформація європейських суспільств зумовила безпрецедентну взаємозалежність між основними правами, технологічною інфраструктурою та регуляторним дизайном. Свобода Інтернету, яка розглядається на перетині приватності, свободи вираження поглядів, доступу до інформації та цифрової рівності, стала структурним елементом демократичного врядування в Європейському Союзі. Однак технології, що покращують комунікацію та участь, одночасно створюють нові форми контролю, нагляду та концентрації влади. Отже,

виклик виходить за межі юридичного визнання цифрових прав і стосується їхньої ефективної реалізації в умовах швидкої технологічної еволюції, політичної поляризації та асиметричної інституційної спроможності. Незважаючи на амбітну нормативну базу ЄС, постійна фрагментація між державами-членами та нерівномірне застосування законодавства продовжують підривати єдиний захист свободи Інтернету. Відповідно, центральна проблема, яка розглядається в цьому дослідженні, полягає у вивченні розбіжності між формальною повнотою архітектури цифрових прав ЄС та її практичним впровадженням у багаторівневій системі управління.

Аналіз останніх досліджень і публікацій. Широке коло вчених досліджувало еволюцію цифрових прав в Європейському Союзі. Теоретики права та інституційні аналітики (А. Бредфорд [2], Дж. Пенні [12]) інтерпретують Хартію основних прав як конституційну основу цифрового врядування, тоді як вчені, що займаються питаннями захисту даних (Ш. Зубофф [13]), розглядають Загальний регламент про захист даних (надалі - GDPR) як парадигмальний зсув у бік моделі регулювання ринку, заснованої на правах. Дослідження Закону про цифрові послуги підкреслюють зусилля ЄС щодо поширення цієї логіки на відповідальність платформ та прозорість алгоритмів. Судова практика Суду Європейського Союзу та Європейського суду з прав людини [10] посилила гарантії конфіденційності та свободи вираження поглядів, тоді як інституційні звіти та аналізи громадянського суспільства викривають постійні асиметрії в застосуванні законодавства ЄС [11]. Проте, незважаючи на багату доктринальну та політичну літературу, ця сфера залишається фрагментованою: приватність, свобода вираження поглядів та регулювання платформ часто розглядаються як окремі питання, а не як взаємозалежні компоненти інтегрованої правової екосистеми. Таке аналітичне розділення обмежує можливість концептуалізувати свободу Інтернету як цілісну конституційну цінність, а не як набір секторальних політик.

Виділення невирішених раніше частин загальної проблеми. Хоча нормативні та правові засади свободи в Інтернеті добре задокументовані, залишається кілька аналітичних прогалин. Існуючі дослідження недостатньо досліджують, як відмінності в адміністративному потенціалі та політичній волі серед держав-членів перетворюються на асиметрію в правозастосуванні. Складна взаємодія між наглядовими органами, агентствами з захисту даних, координаторами цифрових послуг та наднаціональними радами, залишається недостатньо теоретично обґрунтованою, що призводить до фрагментації структур підзвітності. Лише небагато досліджень інтегрують алгоритмічне управління, регулювання нагляду та модерацію контенту в єдину концептуальну систему, тим самим ігноруючи кумулятивний вплив автоматизованого прийняття рішень на захист прав. Крім того, феномен судового плюралізму – взаємодія між СЄС, ЄСПЛ та національними конституційними судами – не має систематичної оцінки як визначальний фактор узгодженості у захисті цифрових прав. Ці невирішені аспекти свідчать про те, що існуюча література відображає нормативні амбіції ЄС, але не пояснює, чому такі амбіції на практиці призводять до непослідовного і часто недостатнього захисту свободи в Інтернеті.

Формулювання цілей статті (постановка завдання). Ця стаття має на меті здійснити всебічний критичний аналіз нормативних та правових механізмів Європейського Союзу щодо захисту свободи в Інтернеті, оцінивши як їхню внутрішню узгодженість, так і практичну ефективність у рамках багаторівневого управління. Дослідження зосереджується на досягненні таких цілей: (1) з'ясувати конституційні та регуляторні основи цифрових прав в ЄС; (2) оцінити, як судові та адміністративні механізми забезпечують їх дотримання в державах-членах; (3) визначити інституційні, політичні та технологічні чинники, що перешкоджають ефективній реалізації; та (4) запропонувати теоретичні та процедурні реформи, які могли б підвищити підзвітність, координацію та стійкість в управлінні цифровими правами в ЄС. Це покликане забезпечити комплексне розуміння того, як наднаціональні правові системи можуть поєднати динамізм технологічних інновацій із незмінними імперативами конституційного захисту та демократичної легітимності.

Виклад основного матеріалу дослідження. Поява захисту персональних даних як окремої правової та етичної категорії є однією з найглибших трансформацій у сфері прав людини в Європейському Союзі. Право контролювати свої дані, яке більше не обмежується приватною сферою, стало необхідною передумовою індивідуальної автономії, гідності та демократичної участі в цифрову епоху. Європейський Союз став першою наднаціональною організацією, яка закріпила це право як фундаментальне, незалежне від більш широкого права на приватність, тим самим сформувавши те, що вчені назвали «конституціоналізацією інформаційного самовизначення» в межах цифрового врядування [2, 3].

Стаття 8 Хартії основних прав Європейського Союзу прямо гарантує право на захист персональних даних, створюючи нормативний дуалізм поряд зі статтею 7, яка захищає приватне та сімейне життя. Це розмежування демонструє перехід від негативного уявлення про приватність (захист від втручання) до проактивного розуміння захисту даних як інструменту для самовизначення

та самоврядування. Положення вимагає, щоб дані оброблялися справедливо, для конкретних цілей, на підставі згоди або законних підстав і під наглядом незалежного органу, тим самим пов'язуючи законність з інституційною відповідальністю.

Концептуальні основи цього права випливають із судової практики Європейського суду з прав людини (ЄСПЛ) відповідно до статті 8 Європейської конвенції з прав людини. У справі «С. та Марпер проти Сполученого Королівства» ЄСПЛ постановив, що безстрокове зберігання біометричних даних правоохоронними органами, навіть щодо осіб, які не були засуджені, порушує право на приватне життя [10]. Аналогічно, у справі «Digital Rights Ireland проти Міністра комунікацій» [4] Суд Європейського Союзу (СЄС) визнав Директиву про зберігання даних недійсною, створивши потужний прецедент, згідно з яким невмотивований збір даних є несумісним з людською гідністю та демократичними цінностями. Ці рішення створили правову основу для європейської доктрини інформаційного самовизначення.

Поступова еволюція законодавчої архітектури ЄС, від Директиви про захист даних 1995 року до Загального регламенту про захист даних (GDPR) 2016 року, інституціоналізувала новий правовий суб'єкт: суб'єкт даних. Ця концепція переосмислює роль фізичних осіб не лише як пасивних бенефіціарів права на приватність, а як активних правовласників, які мають право на доступ, виправлення, видалення та контроль за поширенням даних. Така переорієнтація відображає філософську трансформацію права на приватність в оперативне право, що дає можливість брати участь у цифровій публічній сфері.

Рішення у справі Google Spain проти AEPD та Маріо Костеха Гонсалеса [5] у 2014 році ще більше закріпило цю зміну, встановивши «право на забуття». Європейський суд підтвердив, що особи можуть вимагати видалення з пошукової видачі результатів, які є невідповідними або більше не є актуальними, навіть якщо вони є фактично точними. Ця судова практика наклала позитивні зобов'язання на приватних посередників, таких як пошукові системи, вказавши, що обов'язки щодо дотримання прав людини можуть поширюватися горизонтально на приватну цифрову економіку. Хоча це рішення є суперечливим з точки зору його наслідків для свободи вираження поглядів, воно підтвердило, що захист персональних даних є не тільки захисним правом, але й правом на контроль над своєю цифровою ідентичністю.

На національному рівні держави-члени ЄС перенесли цю нормативну базу в конституційну та адміністративну практику. Федеральний конституційний суд Німеччини задовго до прийняття GDPR визнав інформаційне самовизначення (informationelle Selbstbestimmung) як прояв людської гідності та конституційний принцип [3]. У Франції Національна комісія з інформатики та свобод (CNIL) взяла на себе проактивну роль у вирішенні питань, пов'язаних із впливом нових технологій на права людини, зокрема, вживши правових заходів проти Clearview AI за незаконні практики розпізнавання облич. Такі події є прикладом внутрішньої узгодженості підходу ЄС, орієнтованого на права людини, та його поширення через адміністративне право.

Формулювання ЄС захисту даних як права людини мало вплив далеко за межами його кордонів, що дало початок тому, що Бредфорд називає «Брюссельським ефектом» [2]. Це явище описує, як суворі регуляторні стандарти ЄС стають де-факто глобальними нормами, оскільки транснаціональні корпорації гармонізують свою практику з законодавством ЄС, щоби зберегти доступ до ринку. Як наслідок, юрисдикції по всьому світу – від Бразилії (LGPD) і Японії (APPI) до Каліфорнії (CPRA) – включили положення, що відображають принципи GDPR. Таке поширення підкреслює подвійну ідентичність ЄС як нормативної сили та регулятора цифрової сфери.

Однак екстериторіальне поширення стандартів ЄС також спричинило трансатлантичні напруження, зокрема зі США. Тоді як законодавство ЄС розглядає захист даних як право людини, засноване на гідності, система США залишається переважно договірною або орієнтованою на споживача. Рішення у справі Schrems II (C-311/18) [6] відображало цю розбіжність: Європейський суд ЄС визнав недійсним угоду про захист конфіденційності між ЄС і США на тій підставі, що практики спостереження США не забезпечували «істотної еквівалентності» гарантіям ЄС. Це рішення підтвердило готовність Суду відстоювати фундаментальні права навіть у чутливих геополітичних контекстах, зміцнивши конституційну автономію захисту даних ЄС.

У цифрову епоху як державні, так і корпоративні суб'єкти все більше покладаються на персональні дані як ресурс для управління та економічної діяльності. Однак розширення масштабів та непрозорість обробки даних викликають фундаментальні занепокоєння щодо законності, необхідності та пропорційності відповідно до Хартії та GDPR. Європейська юриспруденція послідовно наголошує, що збір персональних даних повинен залишатися суто необхідним для законних цілей, і цей принцип був перевірений сучасними формами цифрового спостереження.

У справі Tele2 Sverige AB проти Post-och telestyrelsen та Watson та інших [7] ЄСПЛ постановив, що загальні та нечіткі зобов'язання щодо зберігання даних, накладені державами-членами, порушують статті 7 та 8 Хартії. У рішенні було підтверджено стандарт пропорційності, встанов-

лений у справі Digital Rights Ireland, який визначає, що загальні режими зберігання даних підривають суть права на приватність та захист даних. Незважаючи на це, кілька національних органів влади, зокрема у Франції, Німеччині та Польщі, спробували переосмислити або обійти ці рішення за допомогою галузевих законів та надзвичайних винятків, що відображає постійну напругу між імперативами національної безпеки та основними правами.

Ця напруга поширюється на механізми обміну даними на рівні ЄС, такі як Шенгенська інформаційна система (SIS II), EURODAC та Директива про реєстрацію імен пасажирів (PNR). Критики стверджують, що ці інструменти, хоча і призначені для законного правоохоронного контролю та управління міграцією, дають можливість непропорційного профілювання та збору біометричних даних. В результаті концентрація конфіденційної інформації створює ризик перетворення таких систем на «бази даних підозрюваних», які класифікують осіб без достатнього нагляду або можливості оскарження [9]. У цьому відношенні законодавство ЄС про захист даних служить як захистом, так і випробуванням демократичної відповідальності.

Окрім державних практик, комерціалізація персональних даних приватними корпораціями становить структурну загрозу для людської автономії та демократичної рівності. Модель, яку Шошана Зубофф описує як «капіталізм спостереження» [13], базується на здобутті та монетизації поведінкових даних для прогнозування та впливу на людську поведінку. Великі технологічні компанії (Meta, Alphabet, Amazon, TikTok) керують величезними екосистемами, що інтегрують збір даних, висновки штучного інтелекту та алгоритмічне таргетування, часто без інформованої згоди.

Застосування регуляторних заходів відповідно до GDPR виявило системне недотримання вимог. У 2020 р. CNIL оштрафувала Google на 100 млн євро за розміщення рекламних файлів cookie без дійсної згоди, а в 2022 р. Ірландська комісія з захисту даних наклала штраф у розмірі 405 млн євро на Instagram (Meta) за незаконну обробку даних неповнолітніх. Такі випадки викривають постійний розрив між нормативною базою GDPR та корпоративним тлумаченням «законних інтересів» або механізмів згоди. Більше того, асиметрія влади та знань між платформами та користувачами підриває значущий контроль над особистою інформацією, що призводить до того, що Європейська рада з захисту даних (EDPB) називає «втомою від згоди» [1].

Навіть там, де політика конфіденційності та банери з інформацією про файли cookie нібито інформують користувачів, повсюдна наявність темних шаблонів – оманливих дизайнів інтерфейсу, що впливають на рішення – робить згоду все більш ритуальною. Європейська рада з захисту даних (EDPB) засудила такі маніпулятивні архітектури як примусові механізми, що підривають усвідомлений вибір. Цей структурний примус нормалізує інвазивні практики обробки даних, особливо в мобільних та освітніх середовищах, де відмова від них практично неможлива.

Ефективність захисту даних як фундаментального права залежить від надійності механізмів його забезпечення. Згідно з GDPR, національні органи з захисту даних (DPA) функціонують як незалежні наглядові органи, уповноважені проводити аудит, застосовувати санкції та регулювати діяльність контролерів даних. Стаття 51 зобов'язує кожну державу-члена створити автономний наглядовий орган; стаття 58 надає DPA повноваження з проведення розслідувань та вжиття коригувальних заходів, включаючи штрафи, призупинення обробки та передачу справ до судових органів. На рівні ЄС Європейська рада з захисту даних, до складу якої входять представники всіх DPA та Європейський інспектор з захисту даних (EDPS), координує транскордонне виконання через механізми єдиного вікна та узгодженості (статті 60-65 GDPR).

Інституційна модель має на меті поєднати адміністративну незалежність із транснаціональною узгодженістю. Яскравим прикладом такої скоординованої системи є штраф у розмірі 746 млн євро, накладений Люксембурзьким національним комітетом з захисту даних (CNPD) на Amazon Europe у 2021 р. після скарги, спочатку поданої у Франції. Однак розбіжності залишаються. Такі юрисдикції, як Ірландія та Люксембург, де розташовані штаб-квартири багатьох глобальних технологічних компаній, часто критикують за регуляторну інертність, недостатнє фінансування або політичну небажання протистояти потужним корпораціям. Вчені назвали цей дисбаланс «регуляторним вузьким місцем», де концентрація справ у декількох органах захисту даних уповільнює виконання законодавства та підриває рівність захисту в масштабах ЄС [1].

На відміну від цього, наглядові органи у Франції (CNIL), Німеччині (BfDI) та Італії (Garante per la protezione dei dati personali) прийняли більш рішучі стратегії правозастосування, накладаючи значні штрафи та надаючи детальні рекомендації щодо нових питань, таких як штучний інтелект, біометрія та відстеження місцезнаходження. Таким чином, нерівномірність правозастосування залишається як практичною, так і конституційною проблемою для ЄС, що впливає на єдину реалізацію основних прав.

Хоча GDPR залишається основою глобального захисту даних, його застосування викрило глибокі розбіжності між законодавчими прагненнями

та практичною реальністю. Механізм «єдиного вікна», призначений для оптимізації транскордонного нагляду, навпаки, створив регуляторні перешкоди, особливо в Ірландії та Люксембурзі, де розташовані штаб-квартири багатьох великих платформ. Тривалі розслідування та м'які санкції, такі як відстрочка штрафу в розмірі 1,2 млрд євро проти Meta у 2023 р., ілюструють, як процедурна інерція підриває стримуючий ефект і сприяє корпоративному регуляторному арбітражу [1]. Як наслідок, трансформаційна обіцянка GDPR щодо гармонізованого захисту даних часто розпадається на практиці, залишаючи користувачів по всьому Європейському Союзі з неоднаковим рівнем захисту.

Окрім процедурних невідповідностей, індивідуалізована концепція конфіденційності GDPR недостатньо враховує колективну шкоду, що виникає внаслідок алгоритмічної маніпуляції, політичного мікротаргетингу та системної дискримінації. Ці явища виходять за межі особистої шкоди, загрожуючи демократичній участі та рівності. Як стверджують вчені, приватність необхідно переосмислити як соціальну передумову громадянської автономії, а не як суто індивідуальне право. У цьому контексті капіталізм спостереження залишається домінуючою економічною парадигмою, що монетизує прогнозування поведінки за допомогою непрозорих систем здобуття даних [13]. Результатом цього є «інструментальна влада», яка підриває значущу згоду, чинячи негативний вплив на публічний дискурс та політичне самовираження [12].

Для усунення таких структурних дисбалансів ЄС запровадив низку доповнюючих законодавчих рамок, зокрема Закон про цифрові послуги (DSA), Закон про цифрові ринки (DMA) та майбутній Закон про штучний інтелект. Ці інструменти мають на меті забезпечити прозорість, справедливість та підзвітність на етапі проектування цифрових систем. DSA вимагає розкриття алгоритмів та аудиту ризиків, а DMA обмежує монополістичну поведінку онлайн-«воротарів». Водночас спільна думка Європейської ради з захисту даних та Європейського інспектора з захисту даних щодо Закону про штучний інтелект підкреслює необхідність інтеграції принципів захисту даних та людського нагляду в системи штучного інтелекту з високим рівнем ризику. Заразом ці рамки означають перехід від реактивного правозастосування до превентивного цифрового управління.

Технологічні інновації також стали центральним елементом захисту цифрової автономії. Технології підвищення рівня конфіденційності (PET), включаючи шифрування, анонімізацію, псевдонімізацію та диференційовану конфіденційність, перетворюють правові ідеали GDPR на оперативні заходи захисту. Шифрування «від кінця до кінця» (E2EE) є прикладом такого підходу, оскільки гарантує, що доступ до вмісту повідомлень мають лише сторони, які спілкуються, хоча дискусії щодо «законного доступу» та потенційних «задніх дверей» тривають [8]. Додаткові методи, такі як федеративне навчання, докази з нульовим розкриттям інформації та гомоморфне шифрування, дають змогу аналізувати дані без їхнього розкриття, зміцнюючи баланс між інноваціями та конфіденційністю. Однак для їхнього ефективного впровадження необхідні постійні технічні знання та узгодженість нормативно-правових актів у всьому Союзі.

Зрештою, еволюція захисту даних в ЄС відображає постійну боротьбу за поєднання технологічного прогресу з демократичною відповідальністю. Хоча GDPR створив безпрецедентну основу, засновану на правах, його довгостроковий успіх залежить від інституційної послідовності, транскордонного співробітництва та довіри громадськості. Зближення законодавчих інновацій та технологій, що підвищують рівень конфіденційності, відкриває шлях уперед, але основна проблема залишається: забезпечити, щоб цифрова економіка служила людській автономії, а не перетворювала її на товар. У цьому сенсі європейський проєкт цифрового конституціоналізму залишається незавершеним – його майбутнє залежить від здатності втілити права в коді, на практиці та в управлінні.

Висновки та перспективи подальших розвідок у цьому напрямі. Аналіз показує, що підхід ЄС до свободи Інтернету та захисту даних відображає як передову нормативну базу, так і постійні виклики у її практичній реалізації. ЄС успішно конституціоналізував цифрові права за допомогою таких інструментів, як Хартія основних прав та GDPR, проєктуючи цілісну візію цифрового конституціоналізму. Проте розрив між формальними гарантіями та ефективним виконанням залишається значним. Фрагментовані адміністративні можливості, неоднакова судова практика та структурна домінація приватних цифрових акторів продовжують послаблювати єдине застосування основних прав у всьому Союзі. Таким чином, перетворення захисту даних на живу практику демократичного врядування залишається незавершеним.

У середньостроковій перспективі подальші дослідження повинні зосередитися на механізмах координації та підзвітності в межах багаторівневої архітектури управління ЄС. Порівняльні емпіричні дослідження функціонування національних органів захисту даних, координаторів цифрових послуг та наднаціональних наглядових органів могли б пролити світло на інституційні асиметрії, що впливають на результати правозастосування. Аналогічно, взаємодія між судовими інституці-

ями, Європейським судом справедливості, Європейським судом з прав людини та національнми судами, вимагає глибшого теоретичного аналізу для оцінки впливу судового плюралізму на узгодженість захисту цифрових прав. Такий аналіз дав би змогу більш детально зрозуміти, як нормативна модель ЄС працює на практиці.

Загалом, перспективні дослідження повинні інтегрувати технологічні, етичні та соціально-політичні аспекти в дослідження управління цифровими правами. Швидкий розвиток ШІ, алгоритмічного прийняття рішень та режимів безпеки, вимагає уваги до взаємодії між правами людини та обчислювальними інфраструктурами. Таким чином, майбутні дослідження можуть вивчати, як технології підвищення конфіденційності, алгоритмічний аудит та цифрова грамотність можуть слугувати інструментами демократичної стійкості. Отже, європейська модель може еволюціонувати від реактивного регуляторного порядку до проактивної парадигми технологічного самовизначення, заснованої на конституційних цінностях та колективній автономії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Binding Decision 1/2023 on Meta Data Transfers. *European Data Protection Board* : веб-сайт. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/binding-decision-board-art-65/binding-decision-12023-dispute-submitted_en (дата звернення 15.11.2025)

2. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020. 424 p.

3. BVerfGE 125, 260 – Vorratsdatenspeicherung, Beschluss des Bundesverfassungsgerichts vom 2. März 2010. Bundesverfassungsgericht : веб-сайт. URL: https://www.servat.unibe.ch/dfr/bv125260.html (дата звернення: 07.11.2025)

4. Court of Justice of the European Union, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others, Joined Cases C-293/12 and C-594/12, Judgment of 8 April 2014. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0293 (дата звернення 08.11.2025)

5. Court of Justice of the European Union, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos and Mario Costeja González, Case C-131/12 (2014). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131 (дата звернення 10.11.2025)

6. Court of Justice of the European Union, Schrems II, Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, Judgment of 16 July 2020. URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (дата звернення 09.11.2025)

7. Court of Justice of the European Union, Tele2 Sverige AB v. Post-och telestyrelsen, C-203/15 and Watson and Others, C-698/15 (2016). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0203 (дата звернення 08.11.2025)

8. Data Retention Revisited. *European Digital Rights* : вейб-сайт. URL: https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf (дата звернення 07.11.2025)

9. EDPS Opinion on the use of a computerised system by the European Parliament for the digitalisation of the Plenary and central attendance registers through biometric technology. *EDPS* : веб-сайт. URL: https://www.edps.europa.eu/system/files/2021-03/21-03-29_edps_opinion_ep_computerised_system_biometrics_en.pdf (дата звернення 07.11.2025)

10. European Court of Human Rights, S. and Marper v. United Kingdom, Applications Nos. 30562/04 and 30566/04, Judgment of 4 December 2008. URL: https://hudoc.echr.coe.int/eng?i=001-90051 (дата звернення 10.11.2025)

11. It's not a glitch: how Meta systematically censors Palestinian voices. *Access Now*: веб-сайт. URL: https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/ (дата звернення 02.11.2025)

12. Penney J. W. Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*. 2016. №31(1). P. 117-182.

13. Zuboff S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019. 704 p.

Дата першого надходження рукопису до видання: 25.11.2025
Дата прийнятого до друку рукопису після рецензування: 11.12.2025
Дата публікації: 31.12.2025