УДК 340.12:342.9:004.9(4)(477)
DOI https://doi.org/10.24144/2307-3322.2025.92.1.5

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: ЗАХІДНА ДОКТРИНА ТА СУДОВА ПРАКТИКА

Гаращенко В.В.,
аспірант відділу теорії держави і права,
Інститут держави і права ім. В.М. Корецького
ORCID: 0009-0004-8389-0869
e-mail: V.V.Harashchenko@gmail.com

Гаращенко В.В. Захист персональних даних: західна доктрина та судова практика.

Стаття присвячена теоретико-правовому аналізу становлення та розвитку доктрини захисту персональних даних у західній правовій думці. У роботі обґрунтовується, що право на захист персональних даних еволюціонувало від галузевого інституту інформаційного чи конституційного права до самостійної міждисциплінарної категорії загальної теорії права, яка відображає трансформацію уявлень про природу приватності, автономію особи та позитивні обов'язки держави в цифрову епоху.

Проаналізовано основні етапи формування доктрини – від концепції інформаційного самовизначення Спіроса Сімітіса та інституційного підходу Вольфґанґа Гоффманна-Рієма до сучасних теорій екстериторіальності (Крістофер Кунер, Лі А. Байгрейв) і етико-технологічної відповідальності (Джованні Сартор, Ліліан Едвардс). Особливу увагу приділено тому, як ці ідеї вплинули на формування нормативної моделі Загального регламенту ЄС про захист даних (GDPR) та правових механізмів забезпечення інформаційної автономії особи.

Судова практика Суду ЄС, ЄСПЛ та Верховного Суду розглядається як емпіричне підґрунтя перевірки доктринальних положень, а не як самостійний предмет дослідження. Вона виступає своєрідним індикатором життєздатності теоретичних конструкцій, відповідність реаліям цифрового суспільства та викликам технологічного розвитку. Рішення судів відображають процес практичної конкретизації загальнотеоретичних принципів – пропорційності, легітимності, добросовісності та балансу між публічними й приватними інтересами. Через призму цих рішень простежується, як абстрактні доктринальні концепти набувають нормативного змісту, трансформуючись у правові стандарти поведінки держави, бізнесу та індивіда. Таким чином, судова практика стає важливим механізмом верифікації теоретико-правових ідей, сприяючи їх еволюції та адаптації до динаміки цифрової епохи.

У статті доведено, що захист персональних даних у цифровому суспільстві стає не лише інструментом охорони приватності, а й маркером рівня розвитку правової держави. Автор підкреслює, що розвиток цифрових технологій висуває перед теорією права нові методологічні завдання – осмислення феноменів цифрових прав людини, алгоритмічної етики та інформаційної автономії як категорій, що визначають нову парадигму праворозуміння у XXI столітті.

Ключові слова: персональні дані, GDPR, інформаційне самовизначення, пропорційність, судова практика, цифрова епоха, теорія права.

Harashchenko V.V. Personal data protection: western legal doctrine and judicial practice.

The article offers a theoretical and legal analysis of the formation and development of the doctrine of personal data protection in Western legal thought. It substantiates that the right to personal data protection has evolved from a sectoral institution of information or constitutional law into an independent interdisciplinary category of the general theory of law, reflecting the transformation of ideas about privacy, individual autonomy, and the state's positive obligations in the digital age.

The study traces the main stages in the development of this doctrine – from Spiros Simitis's concept of informational self-determination and Wolfgang Hoffmann-Riem's institutional approach to contemporary theories of extraterritoriality (Christopher Kuner, Lee A. Bygrave) and ethical-

technological responsibility (Giovanni Sartor, Lilian Edwards). Particular attention is given to how these theoretical ideas influenced the normative model of the EU General Data Protection Regulation (GDPR) and the legal mechanisms for ensuring an individual's informational autonomy.

The case law of the Court of Justice of the European Union (CJEU), the European Court of Human Rights (ECtHR), and the Supreme Court of Ukraine is considered as empirical evidence for testing doctrinal provisions rather than as a separate object of study. Judicial decisions act as indicators of the viability of theoretical constructs and their conformity to the realities of digital society and technological progress. Through these decisions, abstract doctrinal concepts acquire normative content, transforming into legal standards that regulate the behavior of the state, business, and individuals. Thus, judicial practice functions as a mechanism for verifying and refining theoretical and legal ideas, promoting their adaptation to the dynamics of the digital era.

The article concludes that personal data protection in the digital society is not merely a tool for safeguarding privacy but also a marker of the maturity of the rule of law. The author emphasizes that the rapid development of digital technologies poses new methodological challenges for legal theory – rethinking the phenomena of digital human rights, algorithmic ethics, and informational autonomy as categories that define a new paradigm of legal understanding in the twenty-first century.

Key words: personal data, GDPR, informational self-determination, proportionality, judicial practice, digital age, legal theory.

Постановка проблеми. У сучасній теорії держави і права захист персональних даних виходить за межі суто технічного чи інформаційного регулювання і набуває системного, державно-правового осмислення. У цифрову епоху, коли дані стають новою формою влади, а їх контроль – елементом суверенітету, держава зобов'язана забезпечити баланс між приватністю особи, публічними інтересами та вимогами національної безпеки. З точки зору теорії права, ця проблема відображає трансформацію фундаментальних прав і свобод у цифровому середовищі: від права на приватність – до права на інформаційне самовизначення, а також еволюцію публічно-правових обов'язків держави у сфері цифрового управління. Захист персональних даних стає ключовим індикатором правової держави, адже визначає рівень гарантування гідності, свободи волевиявлення та обмеження втручання держави й приватних структур у сферу особистого життя.

Метою дослідження є аналіз впливу цифрових технологій на безпеку персональних даних, визначення ключових міжнародних стандартів та окреслення викликів, що постають перед національними правовими системами, зокрема Україною, у контексті транскордонної цифрової взаємодії. Також дослідження спрямоване на виявлення зв'язку між теоретичними концепціями інформаційного самовизначення та їхнім практичним втіленням у судовій практиці ЄС, ЄСПЛ і Верховного Суду.

Стан опрацювання проблематики. Проблема правового захисту персональних даних досліджувалася як зарубіжними, так і українськими вченими. Серед класичних праць західної правової доктрини варто виокремити дослідження Спіроса Сімітіса [1] та Вольфганга Гоффманна-Рієма [2], що заклали підґрунтя для формування європейської моделі права на інформаційне самовизначення. У центрі сучасної наукової дискусії перебувають питання екстериторіальної дії Загального регламенту про захист даних (GDPR) (Christopher Kuner [3], Lee A. Bygrave [4], Maria Helen Murphy [5]) та виклики, пов'язані з цифровим суверенітетом.

Аспекти впливу GDPR на глобальні цифрові ринки активно аналізуються американськими дослідниками, зокрема Деніелом Солове (Daniel J. Solove) та Полом М. Шварцом (Paul M. Schwartz) [6]. Значний внесок у розвиток теорії та практики захисту даних здійснили такі вчені, як Гелен Ніссенбаум [7], Вудро Харцог [8], Андреас Фріч [9], Даніель Беме та Крістоф Штеффен, які досліджують взаємозв'язок між технологіями, нормативним регулюванням і правами особи в цифрову епоху.

Вивчення західної правової доктрини у сфері захисту персональних даних є особливо актуальним для України, яка перебуває на шляху європейської інтеграції. Врахування положень, принципів і практики імплементації GDPR є необхідною умовою для ефективної адаптації національного законодавства до правових стандартів Європейського Союзу. Водночас в українському дискурсі відчутна потреба в глибокому теоретичному осмисленні концептуального апарату цифрових прав, балансу між правом на приватність і публічним інтересом, а також правових обмежень у сфері національної безпеки.

Виклад основного матеріалу. Захист персональних даних є одним із ключових напрямів розвитку сучасного міжнародного права та європейської інтеграції. Система правового регулювання цієї сфери є багаторівневою і включає як міжнародні угоди, так і вторинне законодавство ЄС. Основними віхами його розвитку стали Конвенція Ради Європи № 108 [10] та GDPR [11], які встановили базові принципи законності, пропорційності, безпеки та справедливості обробки персональної інформації. Європейський суд з прав людини і Суд ЄС у своїй практиці формують стандарти, що забезпечують баланс між правом на приватність та публічним інтересом. Верховний Суд поступово адаптує ці підходи, розтлумачуючи право на захист даних у світлі міжнародних зобов'язань та національної безпеки. Судова практика підтверджує легітимність використання біометричних технологій, визначає межі згоди на обробку даних та розмежовує приватно- і публічно-правові аспекти цифрової ідентифікації.

Вагомий внесок у формування концепції права на інформаційне самовизначення та його взаємозв'язок із конституційними правами особи зробили такі дослідники, як Спірос Сімітіс (Spiros Simitis) та Вольфганг Гоффманн-Рієм (Wolfgang Hoffmann-Riem). Їхні праці стали теоретичним підґрунтям європейської моделі захисту персональних даних**,** яка отримала міжнародне нормативне закріплення у Конвенції Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (1981 р.), модернізованій згодом відповідно до вимог цифрової епохи.

Один із засновників сучасної доктрини захисту персональних даних Спірос Сімітіс зазначав, що ефективна система захисту персональних даних має ґрунтуватися на трьох ключових засадах. По-перше, інституційних гарантіях**,** які передбачають створення незалежних наглядових органів, відповідальних за контроль дотримання законодавства у сфері персональних даних. По-друге, міжнародному регулюванні, що сприяє уніфікації стандартів захисту персональних даних на наднаціональному рівні. По-третє, демократичному вимірі приватності**,** який забезпечує збереження свободи особистості в умовах цифрового суспільства та слугує фундаментом демократичних інститутів.

Ідея Спіроса Сімітіса щодо «інституційного захисту» індивідуальних прав знайшла своє нормативне відображення в Загальному регламенті ЄС із захисту даних (GDPR, Регламент ЄС 2016/679)**,** який закріпив принцип незалежності органів, відповідальних за захист персональних даних. На думку Сімітіса, держава має не лише реагувати на факти порушення приватності, а й несе позитивний обов'язок щодо активного запобігання таким порушенням. Цей підхід згодом підтримали дослідники Джованні Сартор і Ліліан Едвардс**,** які акцентують увагу на необхідності посилення державного контролю за алгоритмічними процесами та забезпечення захисту особи від непрозорого втручання штучного інтелекту**.**

Таким чином, ідеї Спіроса Сімітіса та Вольфґанґа Гоффманна-Рієма заклали підвалини сучасної європейської моделі захисту персональних даних, яка поєднує демократичні цінності, верховенство права та виклики технологічного розвитку. Сформована на цих засадах доктрина стала теоретичним підґрунтям для формування міжнародних стандартів захисту приватності, зокрема в межах Загального регламенту ЄС про захист даних (GDPR), що визначив новий глобальний стандарт у сфері обробки персональної інформації.

Побудовані на ідеях Спіроса Сімітіса та Вольфґанґа Гоффманна-Рієма концепції стали підґрунтям для подальшого розвитку європейської правової доктрини захисту персональних даних. Їхні напрацювання заклали основи для нового покоління дослідників, які переосмислили проблематику захисту даних крізь призму конституційно-правового та міждисциплінарного підходів.

До представників цієї сучасної доктринальної школи належать Орла Лінскі, Пол де Герт, Вагеліс Папаконстантіну та Лі А. Байгрейв. Зазначені автори розвинули концепцію Сімітіса, перенісши акцент дослідження із загального права на приватність на право на захист персональних даних – як фундаментального права, закріпленого у статті 8 Хартії основних прав Європейського Союзу.

Орла Лінскі у своїх працях розглядає захист персональних даних як самостійне фундаментальне право, що має власну структуру, мету та зміст, відмінну від традиційного права на приватність. Пол де Герт підкреслює, що реалізація цього права вимагає досягнення пропорційного балансу між приватними інтересами особи та легітимними цілями суспільства.

Зазначені доктринальні положення авторів знайшли своє відображення у судовій практиці. Так, у справі № 757/22027/22-ц Верховний Суд (у спорі між фізичною особою і АТ КБ «ПриватБанк»

про захист персональних даних) підтвердив правомірність відмови банку у виконанні вимоги позивача щодо знищення його персональних даних. Суд встановив, що відповідно до ст. 15 Закону України «Про захист персональних даних», дані підлягають знищенню, якщо інше не передбачено законом. Водночас ст. 8 Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» зобов'язує суб'єктів первинного фінансового моніторингу, зокрема банки, зберігати інформацію та документи, що стосуються ділових відносин із клієнтом, не менше п'яти років після їх припинення. Верховний Суд дійшов висновку, що дії банку, спрямовані на збереження даних упродовж цього строку, відповідають вимогам законодавства, оскільки вони мають легітимну мету – забезпечення національної безпеки шляхом запобігання та протидії фінансуванню тероризму і легалізації злочинних доходів.

Таким чином, судова практика демонструє, що вимоги публічного інтересу, пов'язані з питаннями міжнародної безпеки та фінансового моніторингу, можуть законодавчо обмежувати право особи на знищення своїх персональних даних, за умови дотримання принципу пропорційності [12].

Зазначена справа є прикладом реалізації принципу пропорційності, про який писав Пол де Герт, наголошуючи, що реалізація права на захист персональних даних потребує збалансування приватних інтересів особи та легітимних цілей суспільства.

Судова практика Європейського Союзу відображає сучасні тенденції розвитку європейського права захисту персональних даних та акцентує увагу на пошуку оптимального балансу між фундаментальним правом на приватність, економічними інтересами суб'єктів господарювання та ефективністю наглядових механізмів, передбачених Регламентом (ЄС) 2016/679 (GDPR). Показовою у цьому контексті є справа *Meta Platforms Ireland v European Data Protection Board* (T-319/24, Загальний суд, 29 квітня 2025 року), у якій розглядалося питання дійсності згоди користувачів у межах бізнес-моделі «consent or pay». Суд відхилив позов компанії Meta, проте наголосив на ключовому значенні принципів добровільності, поінформованості та конкретності згоди, які становлять основу тлумачення статей 4(11) та 7 GDPR [13].

Це рішення демонструє горизонтальну дію (*Drittwirkung*) фундаментального права на захист персональних даних, про яку писала Орла Лінскі. Під горизонтальною дією розуміється, що зазначене право зобов'язує не лише державні органи, а й приватні суб'єкти господарювання дотримуватися стандартів захисту персональних даних та поважати право користувачів на приватність у межах договірних чи комерційних відносин. У справі *Meta* Суд ЄС, по суті, втрутився у приватні комерційні відносини компанії з метою забезпечення належного виконання фундаментального права на захист даних. Було встановлено, що навіть у межах моделі *«consent or pay»* згода користувача на обробку персональних даних має відповідати найвищим стандартам, гарантованим статтею 8 Хартії основних прав Європейського Союзу.

Таким чином, це рішення підтвердило, що право на захист персональних даних має пряму (горизонтальну) дію (*horizontal effect*) і є непорушним у правовідносинах між приватними суб'єктами. При цьому економічні інтереси компаній не можуть автоматично набувати пріоритету над фундаментальними правами особистості.

Відповідно до підходів, яких дотримуються Орла Лінскі та Полде Герта, захист персональних даних є фундаментальним та універсальним правом, що має транскордонний характер. В умовах глобалізації інформаційних потоків і зростання впливу транснаціональних технологічних корпорацій, дослідники зосереджують увагу на механізмах забезпечення ефективного дотримання цього права, особливо за відсутності єдиного міжнародного органу, відповідального за регулювання процесів обробки персональних даних.

Дослідження Лінскі та де Герта формують теоретичну основу для розуміння глобального виміру права на захист персональних даних. Проте подальший розвиток ця концепція отримала у працях Крістофера Кунера та Лі А. Байгрейва, які розвинули ідею «екстериторіальності» права на захист даних, розглядаючи GDPR як нормативну систему глобальної дії, що встановлює єдиний стандарт для суб'єктів обробки інформації незалежно від їх юрисдикційної приналежності. Такий підхід став основою сучасного правозастосування Суду ЄС у справах, пов'язаних із міжнародними передаваннями даних та контролем за діяльністю цифрових платформ.

Ідеї Крістофера Кунера та Лі А. Байгрейва щодо екстериторіальності права на захист персональних даних отримали практичне втілення у прецедентній практиці Суду Європейського Со-

юзу. Суд послідовно розвиває концепцію глобальної дії європейського права, яка закріплює за GDPR статус універсального стандарту у сфері обробки та передавання персональних даних.

У справі *Schrems v Data Protection Commissioner* (C-362/14, 2015) Суд ЄС визнав недійсним механізм Safe Harbour, який регулював передавання персональних даних з ЄС до США. Суд дійшов висновку, що правова система США не забезпечує «еквівалентного рівня захисту» персональних даних громадян ЄС, що становить порушення статей 7, 8 та 47 Хартії основоположних прав ЄС. Це рішення стало ключовим у підтвердженні екстериторіального впливу GDPR та його пріоритету над національними правовими режимами третіх країн [14].

У подальшому рішенні *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (C-311/18, 2020) Суд скасував дію механізму Privacy Shield, посилаючись на аналогічні міркування щодо недостатності рівня захисту персональних даних у США. Рішення остаточно закріпило доктрину глобальної дії GDPR, яку розробив Кунер, згідно з якою будь-які міжнародні трансфери даних мають відповідати стандартам, встановленим законодавством ЄС, незалежно від територіальної юрисдикції отримувача даних [15].

У справі *Bindl v European Commission* (T-354/22, 2023) Суд уперше детально розглянув питання забезпечення адекватного рівня захисту при внутрішньоєвропейському передаванні персональних даних. Суд підкреслив, що навіть інституції Європейського Союзу повинні дотримуватися принципів GDPR, забезпечуючи прозорість і дотримання принципу мінімізації даних, відповідно до статті 5(1)(c) GDPR, яка вимагає, щоб персональні дані були належними, доречними та обмеженими тим, що є необхідним для досягнення цілей обробки. Це рішення демонструє складність практичної імплементації концепції «адекватності», сформульованої Байгрейвом, яка вимагає не лише територіальної, але й інституційної оцінки рівня захисту [16].

Таким чином, аналіз судової практики свідчить, що Суд ЄС поступово утверджує концепцію глобального правового стандарту захисту персональних даних, який виходить за межі територіальної юрисдикції ЄС. Ця тенденція узгоджується з доктриною екстериторіальності, розробленою Кунером і Байгрейвом, та формує нову парадигму міжнародного правового регулювання у цифровому просторі.

Розвиток концепцій глобальної юрисдикції (Крістофер Кунер) та принципу адекватності захисту при транскордонній передачі даних (Лі А. Байгрейв) засвідчує поступовий вихід права Європейського Союзу (ЄС) за межі традиційного територіального виміру. Окреслена тенденція свідчить про формування універсальної архітектури захисту персональної інформації, у межах якої ЄС претендує на встановлення глобальних стандартів цифрової етики та відповідальності.

Паралельно з глобалізацією процесу обробки даних постає інший, більш докорінний виклик – технологічна еволюція, що змінює способи збирання, аналізу та використання персональної інформації. Якщо Кунер і Байгрейв зосереджували увагу на необхідності контролю за просторовим переміщенням даних, то сучасні дослідники – Джованні Сартор, Ліліан Едвардс і Спірос Сімітіс – зосереджують увагу на контролі за використанням даних у часі та цифрових середовищах. На цьому етапі доктринальний дискурс переходить до питань технологічної адаптації права та позитивних зобов'язань держави у забезпеченні ефективного захисту даних. Йдеться вже не лише про заборони чи обмеження (негативні зобов'язання), але й про активні дії держави – створення інституційних, технічних та етичних механізмів, здатних гарантувати реальний контроль над інформаційними процесами в умовах: штучного інтелекту (ШІ); алгоритмічного аналізу; автоматизованого прийняття рішень.

З огляду на те, що алгоритми, біометричні технології та автоматизовані системи набувають вирішального значення у визначенні обсягу та характеру обробки персональних даних, право в сучасній цифровій екосистемі має невідкладно адаптуватися до цих технологічних реалій. Зазначена тенденція знайшла своє відображення у доктринальних розробках Джованні Сартора та Ліліан Едвардс, які обґрунтовують концепцію етико-технологічної відповідальності. Джованні Сартор розглядає *GDPR* не лише як нормативний акт, а як інструмент етичного контролю за автоматизованими рішеннями, що впливають на права людини. Вчений наголошує, що принцип прозорості та людського контролю є ключовими передумовами збереження людської гідності у цифровому середовищі. Разом з тим, Ліліан Едвардс, пропонує динамічну класифікацію чутливих даних, зазначаючи, що категорії персональної інформації мають розширюватися відповідно до технологічних новацій – зокрема, у сфері штучного інтелекту, Big Data та біометрії.

Вищезазначені теоретичні розробки знайшли своє практичне втілення у судовій практиці, що демонструє функціональність і життєздатність сучасних доктринальних підходів. Так, у справах № 420/26651/23 [17] та № 420/14124/23 [18] Верховний Суд підкреслив, що використання Єдиного державного демографічного реєстру (ЄДДР) та біометричних ідентифікаторів є законним і відповідає принципам цифрової ідентифікації та державній політиці у сфері обробки персональних даних. Ці рішення ефективно окреслюють межі права особи на альтернативні форми ідентифікації, підтверджуючи легітимність біометричних технологій у процесі видачі паспортів. Таким чином, судова практика демонструє спробу держави знайти баланс між правом на приватність та державними потребами у сфері цифрової безпеки.

Європейський суд з прав людини у справі *Cracò v. Italy* (№ 30782/18) встановив порушення права на повагу до приватного життя через відсутність належної анонімізації медичних даних у судових реєстрах. Це рішення наочно ілюструє доктрину позитивних зобов'язань, яку ще у 1970-х роках сформулював Спірос Сімітіс, наголошуючи на активному обов'язку держави забезпечувати інформаційну безпеку громадян [19].

Суд Європейського Союзу у справі *Lindenapotheke* (C-21/23) кваліфікував дані про онлайн-замовлення лікарських засобів як дані про стан здоров'я, тим самим розширивши зміст поняття чутливих даних. Це рішення узгоджується з доктриною цифрової етики Ліліан Едвардс, яка вимагає гнучкого й адаптивного тлумачення правових категорій у добу алгоритмічного управління [20].

Таким чином, сучасна правова доктрина й судова практика конвергують у спільному напрямі: право на захист персональних даних перетворюється на динамічну, багаторівневу систему, що поєднує конституційні принципи, глобальні стандарти та технологічну еволюцію. Це свідчить про перехід від реактивної моделі правового регулювання (орієнтованої на заборони *post factum*) до превентивної, етико-орієнтованої парадигми, здатної забезпечити ефективний захист особистості у цифрову епоху.

Висновки. Еволюція доктрини та судової практики захисту персональних даних у праві Європейського Союзу демонструє системний перехід від класичного розуміння приватності до сучасної концепції права на інформаційне самовизначення як самостійного фундаментального права. Така трансформація відображає глибинні зрушення в правовій системі, спричинені цифровізацією суспільних відносин, і має концептуальне значення для теорії держави і права, оскільки засвідчує перехід від індивідуалістичної до інтегративної моделі захисту прав людини, де держава виступає активним гарантом інформаційної безпеки особи.

У межах європейської правової доктрини виокремлюються три провідні напрями розвитку права на захист даних. Правоцентричний підхід (Орла Лінскі, Пол де Герт) утверджує його як фундаментальне і горизонтальне право, що вимагає дотримання принципу пропорційності у співвідношенні приватних і публічних інтересів. Інституційно-глобальний підхід (Спірос Сімітіс, Крістофер Кунер, Лі А. Байгрейв) наголошує на необхідності створення незалежних наглядових органів і розвиває ідею екстериторіальної дії європейського права як універсального стандарту захисту даних. Етико-технологічний напрям (Джованні Сартор, Ліліан Едвардс) формує концепцію державних позитивних зобов'язань щодо забезпечення етичного використання цифрових технологій і штучного інтелекту.

Судова практика ЄС і ЄСПЛ надала цим доктринальним положенням нормативної конкретизації. Рішення Суду ЄС у справах *Schrems I*, *Schrems II* та *Meta Platforms Ireland v. EDPB* утвердили принцип реальної згоди суб'єкта даних і контроль за транскордонними потоками інформації, тоді як рішення ЄСПЛ у справі *Cracò v. Italy* розвинуло концепцію позитивних зобов'язань держави щодо активного захисту приватності. Верховний Суд у справах № 420/26651/23 та № 420/14124/23 сформулював національний стандарт пропорційності між правом на приватність і потребами цифрової безпеки, тим самим забезпечивши поступову інтеграцію європейських стандартів у вітчизняне правозастосування.

З огляду на це, в Україні доцільно посилити інституційні засади захисту персональних даних шляхом створення незалежного наглядового органу; утвердити принцип пропорційності як універсальний критерій допустимості обмеження приватності; а також розробити правові та етичні засади використання штучного інтелекту відповідно до актів ЄС (*AI Act*, *Digital Governance Act*). Реалізація цих кроків сприятиме не лише гармонізації українського законодавства з європейським правом, а й зміцненню сучасної парадигми теорії права, у межах якої інформаційна автономія особи та державна відповідальність за цифрову безпеку постають взаємодоповнювальними елементами правової держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Spiros Simitis. Revisiting Sensitive Data. Strasbourg: Council of Europe, 1999. URL: https://rm.coe.int/16806845af%3E.
2. Гоффманн-Ріем В. *Legal Technology / Computational Law: Preconditions, Opportunities and Risks* / Wolfgang Hoffmann-Riem. URL: https://journalcrcl.org/crcl/article/view/7/3.
3. Кунер К. *Transborder Data Flows and Data Privacy Law* / C. Kuner. – Oxford: Oxford University Press, 2017. URL: https://www.researchgate.net/publication/ 259994485_Transborder_Data_Flows_and_Data_Privacy_Law.
4. Байгрейв Л. *Data Protection Law: Approaching its Rationale, Logic and Limits* / L.A. Bygrave. Oxford: Oxford University Press, 2020. URL: https://www.researchgate.net/publication/220668128_Data_Protection_Law_Approaching_its_Rationale_Logic_and_Limits_by_L_A_Bygrave.
5. Murphy M.H. Assessing the Implications of Schrems II for EU–US Data Flow. International & Comparative Law Quarterly, Vol. 71, Issue 1, 2022, pp. 245-262. DOI: 10.1017/S0020589321000348. URL: https://www.researchgate.net/publication/355085299_ ASSESSING_THE_IMPLICATIONS_OF_SCHREMS_II_FOR_EU-US_DATA_FLOW.
6. Solove, D.J., & Schwartz, P.M. (2014). *Reconciling personal information in the United States and European Union*. California Law Review, 102(4), 877–916. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442.
7. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life / H. Nissenbaum. Stanford: Stanford University Press, 2010). Джулі Е. Коен (Cohen J.E. Configuring the Networked Citizen / J. E. Cohen.2012. URL: https://scholarship.law.georgetown.edu/cgi/ viewcontent.cgi?article=1826&context=facpub.
8. Hartzog W. Privacy's Blueprint: The Battle to Control the Design of New Technologies / W. Hartzog. Cambridge, MA: Harvard University Press, 2018.), Омер Тене (Tene O. Privacy in the Age of Big Data: A Time for Big Decisions / O. Tene. 2012. URL: https://www.researchgate.net/publication/259892061_Privacy_in_the_Age_of_Big_Data_A_Time_for_Big_Decisions.
9. Фріч А. Privacy Control Patterns for Compliant Application of GDPR. 2019. 9 с. URL: https://www.researchgate.net/publication/335210733_Privacy_Control_Patterns_for_Compliant_Application_of_GDPR.
10. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (1981 р.) URL: https://zakon.rada.gov.ua/laws/show/994_326.
11. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) / Європейський Парламент і Рада ЄС. URL: https://gdpr-text.com/uk.
12. Постанова Верховного Суду від 29 листопада 2023 року у справі № 757/22027/22-ц (провадження № 61-13409св23). URL: https://reyestr.court.gov.ua/Review/115423807.
13. General Court of the European Union (T 319/24, Meta Platforms Ireland Ltd v European Data Protection Board), Постанова (Десята палата) від 29 квітня 2025 р. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=298762&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=200344
14. Court of Justice of the European Union (CJEU), Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, Judgment of 6 October 2015. URL: https://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN.
15. Court of Justice of the European Union (CJEU), Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, Judgment of 16 July 2020. URL: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN.
16. General Court of the European Union (T 354/22, Thomas Bindl v European Commission), Ухвала від 8 січня 2025 р. URL: https://curia.europa.eu/juris/document/ document.jsf?docid=294090&doclang=EN.
17. Постанова Верховного Суду від 06 лютого 2025 року у справі № 420/26651/23 (провадження № К/990/16336/24). URL: https://reyestr.court.gov.ua/Review/125011966.
18. Постанова Верховного Суду від 06 лютого 2025 року у справі № 420/14124/23 (провадження № К/990/15489/24). URL: https://reyestr.court.gov.ua/Review/125011971.

19. Cracò v Italy (№ 30782/18) European Court of Human Rights, Judgment of 13 June 2024. URL: https://hudoc.echr.coe.int/eng#{%22appno%22:[%2230782/18%22]}.
20. Lindenapotheke (C 21/23) Court of Justice of the European Union, Judgment of 4 October 2024. URL: https://curia.europa.eu/juris/document/document.jsf?text=&docid=290696& pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=2925415.