КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА
ФАКУЛЬТЕТ ПРАВА ТА МІЖНАРОДНИХ ВІДНОСИН

Кафедра міжнародного права, європейської та
євроатлантичної інтеграції

Спеціальність 293 «Міжнародне право»
Освітня програма 293.00.01 «Міжнародне право»

БАКАЛАВРСЬКА РОБОТА
на тему:

ЦИФРОВА ПРИВАТНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ: МІЖНАРОДНО-ПРАВОВІ МЕХАНІЗМИ У КОНТЕКСТІ КІБЕРБЕЗПЕКИ ТА ПРАВ ЛЮДИНИ

Здобувачки IV курсу
першого (бакалаврського) рівня вищої освіти
денної форми навчання
Яким'юк Софії Миколаївни

Науковий керівник –
Тітко Е.В., професор кафедри міжнародного права,
європейської та євроатлантичної інтеграції, д. ю. н., доцент,

Київ – 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ГА ООН	Генеральна Асамблея Організації Об'єднаних Націй
ЄКПЛ	Європейська конвенція з прав людини
ЄС	Європейський Союз
ЄСПЛ	Європейський суд з прав людини
ЗМІ	Засоби масової інформації
ЗУ	Закон України
ККУ	Кримінальний кодекс України
Конвенція 108+	Конвенція Ради Європи №108+ «Про захист осіб у зв'язку автоматизованою обробкою персональних даних»
КУ	Конституція України
КУпАП	Кодекс України про адміністративні правопорушення
МПГПП	Міжнародний пакт про громадські і політичні права
ОЕСР	Організація економічного співробітництва та розвитку
ООН	Організація Об'єднаних Націй
РЄ	Рада Європи
Суд ЄС	Суд Європейського Союзу
ЦКУ	Цивільний кодекс України
ШІ	Штучний інтелект
EU AI Act	Регламент Європейського Союзу про встановлення гармонізованих правил щодо Штучного інтелекту (EU Artificial Intelligence Act)
GDPR	Загальний регламент про захист даних (General Data Protection Regulation)

ВСТУП

Актуальність: Процеси глобальної цифровізації суспільства зумовили трансформацію традиційних уявлень про межі приватного життя та засоби його правового забезпечення. В умовах стрімкого розвитку інформаційно-комунікаційних технологій, кіберінфраструктури та штучного інтелекту персональні дані набули статусу окремого об’єкта правовідносин, що має не лише індивідуальну, але й значну суспільну, економічну та політичну цінність. Відповідно, питання цифрової приватності виходить за межі національного регулювання та набуває глобального, міжнародно-правового характеру.

Права людини, гарантовані універсальними й регіональними міжнародними актами, зокрема право на повагу до приватного і сімейного життя, закріплене у статті 12 Загальної декларації прав людини 1948 року (далі – Декларація) [75], статті 17 Міжнародного пакту про громадянські і політичні права 1966 року (далі – МПГПП, Пакт) [56] та статті 8 Європейської конвенції з прав людини 1950 року (далі – ЄКПЛ) [46], постають у новому контексті — контексті цифрової взаємозалежності держав, суспільства та особи. Масове використання технологій обробки даних, глобальні інформаційні потоки та активна діяльність транснаціональних корпорацій, що володіють величезними масивами персональної інформації, створюють нові виклики для реалізації та ефективного захисту права на приватність.

Особливої актуальності набуває проблема забезпечення належного балансу між охороною персональних даних та гарантуванням кібербезпеки. В умовах постійного зростання кількості кібератак, витоків даних і випадків несанкціонованого доступу до інформації з боку як приватних суб’єктів, так і державних структур, постає потреба у створенні комплексних міжнародно-правових механізмів, здатних забезпечити ефективний контроль та відповідальність у цифровому просторі. Кібербезпека та право на приватність дедалі більше розглядаються як взаємопов’язані елементи єдиної системи захисту прав людини у цифрову добу.

Для України питання захисту персональних даних є надзвичайно важливим у світлі процесів європейської інтеграції та гармонізації національного законодавства

із правом Європейського Союзу. Особливого значення ця проблематика набуває в умовах повномасштабної збройної агресії російської федерації, що супроводжується активним використанням кіберзасобів у гібридній війні. Систематичні кібератаки на державні інформаційні ресурси, злами реєстрів, витоки персональних даних громадян, кібершпигунство та поширення дезінформації становлять реальну загрозу не лише приватності людини, але й національній безпеці України. У нинішніх умовах сьогодення, формування ефективної системи правового захисту персональних даних відповідно до міжнародних стандартів набуває не лише юридичного, а й стратегічного значення — як елемент забезпечення інформаційного суверенітету, кіберстійкості та захисту прав людини навіть у період воєнного стану.

Міжнародні організації — ООН, Рада Європи, Європейський Союз — уже розробили низку базових правових інструментів у дані сфері, серед яких ключове місце займають Конвенція Ради Європи №108+ «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» (далі – Конвенція 108+) та Загальний регламент ЄС про захист даних (далі – GDPR, Регламент) [64]. Дані документи встановлюють високі стандарти забезпечення приватності, що стали орієнтиром для національних законодавств багатьох держав. Їх імплементація в українське правове поле є важливим чинником подальшої інтеграції України до європейського правового простору.

Аналіз проблем цифрової приватності неможливий без врахування **наукових досліджень** зарубіжних та українських вчених, які зосереджуються на правових аспектах цифрових технологій. Зокрема, значний внесок у розвиток відповідної проблематики здійснили Воррен С. та Брандейс Л., які заклали концептуальні основи права на приватність; Вестін А., який розробив теорію інформаційного самовизначення особи; Солове Д. молодший, який сформував сучасну таксономію порушень приватності в цифровому середовищі; Ніссенбаум Г., авторка концепції контекстуальної цілісності інформаційних потоків; Зубофф Ш., яка дослідила механізми цифрового стеження як нову форму влади; Байґрейв Л., який системно проаналізував міжнародно-правові засади захисту персональних даних, а також Дюген С. та інші, які досліджують вплив цифрових технологій на правові системи та

права людини. В українській правовій науці питання захисту персональних даних і цифрових прав розгядаються численною кількістю вчених та практикуючих юристів, наприклад, як Брижко В., Ваганова І., Гнатюк С., Жуляєв В., Кокарча Ю., Пилипчук В., Тищук Н., Харитонов Є. та інші.

Мета бакалаврської роботи полягає у здійсненні міжнародно-правового аналізу механізмів захисту цифрової приватності та персональних даних у контексті кібербезпеки та прав людини.

Виходячи з поставленої мети в даній бакалаврській роботі, до виконання виходять наступні **завдання:**

– проаналізувати теоретико-правові засади права на цифрову приватність;

– дослідити історичний розвиток права на приватність у міжнародному праві;

– визначити вплив сучасних кіберзагроз та технологій штучного інтелекту на реалізацію права на приватність;

– дослідити міжнародно-правові стандарти захисту персональних даних;

– проаналізувати практику Європейського суду з прав людини щодо цифрової приватності;

– встановити міжнародно-правові механізми контролю та відповідальності у даній сфері;

– визначити стан імплементації міжнародних стандартів захисту персональних даних у правову систему України та окреслити перспективи гармонізації національного законодавства з *acquis communautaire* Європейського Союзу.

Об’єкт дослідження: суспільні правовідносини у сфері міжнародно-правового захисту цифрової приватності та персональних даних.

Предмет дослідження: міжнародно-правові норми та стандарти, механізми та практика забезпечення захисту персональних даних і цифрової приватності загалом.

Методи дослідження: методологічну основу роботи становить система загальнонаукових та спеціально-юридичних методів, зосібна:

У першому розділі було використано: метод аналізу та синтезу, історико-правовий метод, порівняльно-правовий метод.

У другому розділі були застосовані такі методи: формально-юридичний метод, метод тлумачення правових норм, метод юридичної інтерпретації , порівняльний метод, системно-аналізуючий метод.

У третьому розділі було використано такі методи: системно-структурний метод, аналітичний метод, метод правового прогнозування та метод узагальнення.

Апробація: основні аспекти дослідження були апробовані у двох тезах доповідей на наукових конференціях:

1. «Захист персональних даних в умовах воєнного стану в Україні: виклики цифрової безпеки та міжнародні стандарти» Всеукраїнська науково-практична конференція (XI Круглий стіл) «Права людини в умовах воєнного стану в Україні» 2025 року [20].
2. «Захист права на приватність у цифровому середовищі: аналіз практики ЄСПЛ» III студентська наукова конференція «Міжнародне та публічне право: перспективи та виклики» 2026 року [21].

Структура роботи: бакалаврська робота складається з переліку умовних скорочень, вступу, трьох розділів, які включають дев’ять підрозділів, висновків, списку використаних джерел (77 найменувань) та одного додатку. Загальний обсяг роботи – 97 сторінок.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ЦИФРОВОЇ ПРИВАТНОСТІ ТА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МІЖНАРОДНОМУ ПРАВІ

1.1. Право на повагу до приватного життя як фундаментальна основа захисту цифрової приватності в міжнародному праві прав людини.

На сучасному етапі еволюції міжнародного права прав людини право на приватне життя розглядається як одна з визначальних основ забезпечення особистої автономії, поваги до людської гідності та недоторканності приватної сфери в умовах цифровізації суспільних відносин.

Умови цифрової трансформації суспільства, що характеризуються масштабною інформатизацією, автоматизацією процесів обробки даних та глобалізацією інформаційних потоків, зумовлюють якісне переосмислення змісту приватності як правової категорії. Відповідні процеси свідчать про еволюцію класичного розуміння приватного життя від традиційно фізичного та сімейного виміру до комплексної інформаційної моделі, що охоплює цифрову ідентичність особи та її поведінку у віртуальному середовищі.

У науково-правовій доктрині міжнародного права приватність розглядається як фундаментальна складова концепції людської гідності, що передбачає можливість особи самостійно визначати межі доступу до інформації про себе, контролювати процеси її поширення та забезпечувати недоторканність власного інформаційного простору. Формування відповідного підходу стало результатом тривалого розвитку універсальних і регіональних стандартів прав людини, у межах яких особливу роль відіграла діяльність Організації Об’єднаних Націй (далі – ООН) та Рада Європи (далі – РЄ), що сприяли інституціоналізації права на повагу до приватного життя як самостійного об’єкта міжнародно-правового регулювання.

Сучасний етап розвитку інформаційного суспільства характеризується появою принципово нових ризиків для приватності, пов’язаних із використанням технологій великих даних, алгоритмічного аналізу інформації, штучного інтелекту (далі – ШІ) та цифрових платформ. Такі процеси обумовлюють необхідність адаптації традиційних

правових механізмів до умов цифрового середовища, що, у свою чергу, призводить до формування концепції цифрової приватності як окремого напряму міжнародно-правового регулювання. Зазначений контекст демонструє, що цифрова приватність постає не як нове право, а як еволюційне продовження класичного права на повагу до приватного життя, трансформованого відповідно до технологічних змін сучасності. Водночас у сучасній міжнародно-правовій доктрині все більшого поширення набуває концепція «*цифрових прав*» (англ.: *digital rights*), яка відображає трансформацію змісту класичних прав людини в умовах цифровізації. У періодичних резолюціях Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» [74] послідовно наголошується, що держави несуть не лише негативні зобов'язання утримуватися від свавільного втручання у праватне життя, але й позитивні обов'язки щодо забезпечення ефективного захисту осіб від втручань з боку третіх суб'єктів, зокрема транснаціональних технологічних компаній.

Теоретичне осмислення права на приватність ґрунтується на багатовимірній концепції особистої автономії, яка включає фізичний, інформаційний, комунікаційний та просторовий компоненти. Такий підхід відображає сучасну тенденцію до розширення змісту приватності через інтеграцію інформаційного аспекту, що набуває ключового значення в умовах цифровізації суспільних відносин. Інформаційна приватність у даному випадку розглядається як здатність особи здійснювати контроль над персональними даними, включаючи їх збирання, обробку, зберігання та транснаціональну передачу.

Нормативне закріплення права на повагу до приватного життя стало фундаментом для формування міжнародних стандартів захисту персональних даних. Міжнародна практика поступово виробила концепцію, відповідно до якої ефективний захист приватності неможливий без встановлення чітких правових принципів обробки персональних даних, зокрема принципів законності, пропорційності, мінімізації даних, цільового обмеження та підзвітності суб'єктів обробки інформації. Вказані принципи формують сучасну модель правового регулювання цифрової приватності та визначають напрям подальшого розвитку міжнародного права у цій сфері.

Важливий вплив на становлення сучасного розуміння приватності здійснили класичні доктринальні підходи, сформульовані наприкінці XIX століття. Значний внесок у розвиток відповідної концепції здійснили американські правники Самуель Воррен та Луїс Брандейс, які у своїй науковій роботі «The Right to Privacy» [76] (1890) опублікованій у Harvard Law Review, обґрунтували необхідність формування самостійного правового інституту захисту приватної сфери особи. Написання праці було зумовлене соціально-технологічними змінами другої половини XIX століття, зокрема стрімким розвитком масової преси, фотографії та інших засобів поширення інформації, що значно розширили можливості втручання у приватне життя людини.

У своїй роботі автори запропонували концепцію права особи на недоторканність приватної сфери, сформулювавши відоме визначення приватності як «*right to be let alone*» — права людини бути залишеною у спокої. На їхню думку, традиційні правові механізми захисту власності або честі та гідності були недостатніми для забезпечення належного рівня захисту особистого життя, оскільки нові технології створювали принципово інші форми посягання на особисту сферу. У зв'язку з цим Воррен і Брандейс запропонували розглядати приватність як окреме суб'єктивне право, спрямоване на забезпечення контролю особи над поширенням інформації про її особисте життя.

Запропонована ними концепція мала значний вплив на подальший розвиток правової доктрини та судової практики, насамперед у праві США, де поступово сформувалося розуміння приватності як одного з фундаментальних аспектів особистої свободи. У подальшому ідеї Воррена і Брандейса стали підґрунтям для розвитку ширшої концепції інформаційної автономії особи, яка передбачає право людини контролювати обіг інформації про себе та визначати межі її поширення.

З розвитком інформаційних технологій у XX–XXI століттях ця доктринальна концепція набула нового значення, трансформувавшись у сучасні правові підходи до регулювання захисту персональних даних. Саме на її основі поступово сформувалася ідея інформаційного самовизначення особи, що стала важливим елементом міжнародних та регіональних стандартів захисту приватності. Таким чином, класичні доктринальні положення, сформульовані наприкінці XIX століття, заклали

методологічні основи сучасного правового розуміння приватності та суттєво вплинули на формування міжнародно-правових механізмів захисту персональних даних у цифрову епоху.

Подальші витоки розвитку сучасного розуміння приватності пов'язані з науковими дослідженнями Алана Вестіна, який запропонував розглядати приватність як процесуальну та змінну категорію, що відображає здатність особи контролювати обіг інформації про себе в умовах розвитку інформаційного суспільства. Відповідні концептуальні підходи найбільш системно викладено у його фундаментальній праці «Privacy and Freedom» [77] (1967 р.). Учений підкреслював, що приватність не є статичним станом ізоляції, а виступає механізмом балансування між необхідністю соціальної взаємодії та потребою збереження особистої автономії. Такий підхід заклав теоретичні засади сучасного розуміння інформаційної автономії особи та суттєво вплинув на формування міжнародних стандартів захисту персональних даних у контексті цифровізації суспільних відносин.

Сформульована ним концепція інформаційного самовизначення (*informational self-determination)* заклала теоретичні засади сучасного підходу до правового регулювання обробки персональних даних. Відповідно до неї, ключовим елементом приватності визнається право особи самостійно визначати умови доступу до власної інформації, а також контролювати її використання різними суб'єктами.

Вказаний підхід набув широкого розвитку у міжнародній правовій доктрині та став концептуальною основою формування сучасних міжнародних стандартів захисту персональних даних, зокрема в умовах цифрової трансформації правовідносин та зростання ролі автоматизованих технологій обробки інформації.

У міжнародно-правовому вимірі право на повагу до приватного життя функціонує як інтегративна категорія, що перебуває у взаємозв'язку з іншими фундаментальними правами людини, зокрема свободою вираження поглядів, правом на ефективний засіб юридичного захисту та принципом верховенства права. Особливого значення набуває проблема забезпечення балансу між приватністю та публічними інтересами, що є однією з ключових дилем сучасного міжнародного права в умовах розвитку цифрових технологій та інформаційних платформ.

Визначальний вплив на формування сучасного змісту права на приватність здійснила практика Європейського суду з прав людини (далі – ЄСПЛ, Суд), який розвинув доктрину еволюційного тлумачення міжнародно-правових норм на основі концепції «*живого інструменту*». У межах відповідної практики поняття «*приватне життя*» отримало значно ширше трактування та було поширене на сферу електронних комунікацій, цифрової ідентичності, обробки біометричних даних і захисту персональної інформації у мережі Інтернет. Суд також сформулював принцип позитивних зобов'язань держав щодо забезпечення ефективних правових механізмів захисту персональних даних, що стало важливим етапом розвитку міжнародних стандартів цифрової приватності.

В умовах цифровізації глобального простору суттєвий вплив на розвиток правового регулювання приватності здійснює правова система Європейського Союзу (далі – ЄС, Союз), у межах якої сформовано комплексну модель захисту персональних даних як складової права на повагу до приватного життя. Європейський підхід характеризується системністю, високим рівнем нормативної деталізації та орієнтацією на забезпечення реального контролю особи над власними даними. Відповідна модель поступово набуває глобального значення та впливає на гармонізацію міжнародних стандартів у сфері цифрової приватності.

Таким чином, право на повагу до приватного життя виступає фундаментальною концептуальною та нормативною основою формування сучасної системи міжнародно-правового захисту цифрової приватності. Еволюція інформаційного суспільства, розвиток цифрових технологій та транснаціональний характер обігу персональних даних обумовлюють подальше розширення змісту відповідного права, що потребує системного вдосконалення міжнародних правових механізмів та адаптації традиційних підходів до нових технологічних реалій. У даному контексті цифрова приватність поступово трансформується у ключовий елемент сучасної архітектури прав людини, визначаючи напрям розвитку міжнародного права у XXI столітті.

1.2. Історичний розвиток та еволюція підходів до права на приватність у міжнародно-правовому контексті.

Право на приватність у сучасному міжнародному праві розглядається як одна з фундаментальних гарантій забезпечення прав і свобод людини. Водночас формування його міжнародно-правової доктрини відбувалося поступово та відображало загальну еволюцію уявлень про межі особистої автономії індивіда у суспільстві. Історичний розвиток права характеризується послідовним розширенням його змісту — від ранніх правових уявлень про недоторканність особи, житла та приватного життя до формування комплексного правового режиму інформаційної приватності та захисту персональних даних.

У міжнародно-правовому контексті становлення права на приватність супроводжувалося поступовим ускладненням механізмів його забезпечення під впливом трансформації міжнародних відносин, розвитку інформаційних технологій та формування універсальної системи захисту прав людини. Сучасне розуміння права на приватність сформувалося внаслідок поетапного нормативного закріплення відповідних гарантій як на універсальному, так і на регіональному рівнях міжнародного права, що зумовило його перетворення на одну з ключових складових сучасної правової системи захисту прав людини.

Витоки сучасного розуміння права на приватність простежуються ще у правових конструкціях античності, насамперед у праві Давнього Риму. Хоча римська правова система не оперувала категорією приватності у сучасному значенні цього терміну, окремі деліктні механізми забезпечували захист особистої сфери людини від неправомірного втручання. Зокрема, важливу роль відігравав делікт *actio iniuriarum,* спрямований на захист немайнових інтересів особи, таких як честь, гідність, тілесна недоторканність та соціальна репутація. Застосування відповідного позову передбачало можливість притягнення до відповідальності за дії, які посягали на особисту сферу індивіда або принижували його гідність у суспільстві [1, 18].

У процесі еволюції римського права зміст делікту *iniuria* поступово розширювався: від первісного розуміння як фізичної образи до більш широкого трактування, що охоплювало різні форми посягання на особисту гідність та

соціальний статус особи. Преторська практика сприяла розвитку відповідних механізмів правового захисту, визнаючи можливість притягнення до відповідальності не лише за фізичні посягання, але й за дії, які завдавали моральної шкоди або порушували соціальну повагу до особи [1, 18]. У такий спосіб римська правова традиція фактично сформувала раннє уявлення про необхідність правового захисту немайнових аспектів людської особистості, що згодом стало важливим підґрунтям для формування інституту особистих немайнових прав у європейській правовій традиції.

Подальший розвиток відповідних ідей відбувався в європейській правовій думці Нового часу. У період Просвітництва концепція індивідуальної автономії поступово утвердилася як фундаментальний принцип організації суспільства та водночас як межа допустимого втручання державної влади у сферу особистого життя. Ідеї природного права, індивідуальної свободи та недоторканності особи сприяли формуванню уявлення про існування особливої приватної сфери людського життя, яка повинна бути захищена від надмірного державного чи суспільного контролю.

Важливим етапом подальшого розвитку доктрини приватності стало формування наприкінці XIX століття наукових підходів, спрямованих на виокремлення приватності як самостійної правової категорії. З огляду на праці, розглянуті раніше, значну роль у цьому процесі відіграв попередньою згаданий ессей Самуеля Воррена та Луїса Брандейса — «The Right to Privacy» [76], який став важливою віхою у формуванні наукових уявлень про необхідність правового захисту приватної сфери особи в умовах розвитку засобів масової комунікації. У зазначеній роботі було закладено теоретичні передумови для подальшого осмислення приватності як самостійного об’єкта правового захисту та окреслено напрями подальшої еволюції відповідної правової доктрини.

Початковий етап міжнародно-правового оформлення права на приватність пов’язаний із діяльністю Організації Об’єднаних Націй після завершення Другої світової війни. У контексті формування універсальної системи гарантій прав людини міжнародне співтовариство розпочало процес кодифікації базових стандартів захисту основоположних прав і свобод особи. В умовах необхідності створення глобальної

системи гарантій прав людини необхідним кроком стало прийняття в 1948 році Загальної декларації прав людини [75], яка заклала фундаментальні стандарти охорони приватної сфери. Відповідно до статті 12 Декларації забороняється свавільне або незаконне втручання в особисте і сімейне життя, недоторканність житла та таємницю кореспонденції, а також посягання на честь і репутацію особи. Крім того, норма встановлює право кожної людини на ефективний правовий захист від подібних втручань. Подальший розвиток нормативного закріплення права на приватність на універсальному рівні пов'язаний із прийняттям у 1966 році Міжнародного пакту про громадянські і політичні права [56], який трансформував раніше сформульовані міжнародні стандарти у юридично обов'язкові міжнародно-правові зобов'язання держав.

Відповідно до статті 17 Пакту [49] встановлюється заборона свавільного або незаконного втручання у приватне і сімейне життя особи, її житло та кореспонденцію, а також незаконних посягань на честь і репутацію. Крім того, кожній особі гарантується право на правовий захист від таких втручань або посягань. У такий спосіб положення Пакту розвивають принципи, закріплені раніше у Загальній декларації прав людини [75], надаючи їм обов'язкової сили в межах міжнародного договірного права.

Водночас значення статті 17 слід розглядати у взаємозв'язку з положеннями статті 2 Пакту [56], яка визначає загальні зобов'язання держав-учасниць щодо забезпечення прав і свобод, передбачених цим міжнародним договором. Згідно з зазначеною нормою держави зобов'язані поважати та гарантувати права людини, а також вживати необхідних законодавчих та інших заходів для їх реалізації та ефективного захисту.

У практиці Комітету ООН з прав людини подальший розвиток тлумачення права на приватність відображено у загальних коментарях до Міжнародного пакту про громадянські і політичні права. Зокрема, у Загальному коментарі №16 [29] Комітет конкретизував, що поняття приватного життя охоплює фізичну та психологічну недоторканність особи, захист персональних даних та інші аспекти індивідуальної автономії, а будь-яке втручання у приватну сферу повинно

відповідати критеріям законності, необхідності та пропорційності. Проте, у Загальному коментарі №34 [49] підкреслено необхідність забезпечення балансу між правом на приватність і свободою вираження поглядів, зокрема у контексті діяльності засобів масової інформації (далі – ЗМІ) та сучасних цифрових платформ.

Важливим етапом розвитку універсальних стандартів стало прийняття у 1980 році Керівних принципів Організації економічного співробітництва та розвитку щодо захисту приватності та транскордонних потоків персональних даних [52], які сформували першу міжнародну модель регулювання обробки персональних даних у глобальному економічному середовищі. Керівні принципи ОЕСР закріпили ключові принципи інформаційної приватності, серед яких обмеження збору даних, визначеність мети обробки, забезпечення безпеки інформації, принцип відкритості та відповідальність суб'єктів обробки персональних даних. Зосібна, до них належать:

1. Принцип законності та справедливості збору даних (англ.: *lawfulness and fairness*) – персональні дані повинні збиратися законними способами та без порушення прав і свобод особи.

2. Принцип визначеності мети (англ.: *purpose specification*) – збір персональних даних може здійснюватися виключно для конкретно визначених, правомірних цілей, а їх подальша обробка не повинна суперечити таким цілям або виходити за їх межі.

3. Принцип точності даних (англ.: *data accuracy*) – забезпечення точності, актуальності персональних даних, а також їх своєчасного оновлення у разі потреби.

4. Принцип обмеження строків зберігання (англ.: *storage limitation*) – персональні дані можуть зберігатися лише протягом періоду, необхідного для реалізації мети їх обробки.

5. Принцип доступу суб'єкта даних (англ.: *individual participation*) – право бути поінформованим про обробку персональних даних, отримувати доступ до них, а також ініціювати їх виправлення чи видалення у випадках, передбачених законодавством [52].

Міжнародні договори у сфері захисту окремих категорій прав людини також закріплюють відповідні стандарти поваги до приватної сфери. Так, Конвенція про

права дитини 1989 року [35] у статті 16 встановлює право дитини на захист від свавільного або незаконного втручання в її приватне життя, сім'ю, житло чи особисті комунікації, а також від протиправних посягань на честь і репутацію. Положення формує спеціальні гарантії охорони приватності дітей, які мають враховуватися у діяльності державних органів, освітніх установ та інших інституцій, зокрема в умовах функціонування цифрового інформаційного середовища.

Важливі стандарти у даній сфері закріплені також у Конвенції про права осіб з інвалідністю 2006 року [34] . Відповідно до статті 22 держави-учасниці зобов'язані забезпечувати повагу до приватного життя осіб з інвалідністю, включаючи конфіденційність їхньої особистої, медичної та реабілітаційної інформації, а також гарантувати рівний і недискримінаційний доступ до ефективних засобів правового захисту.

Окремі аспекти охорони приватної сфери відображені й у Міжнародній конвенції про захист прав усіх трудящих-мігрантів і членів їхніх сімей 1990 року [55], яка поширює гарантії на недоторканність приватного та сімейного життя, захист особистих повідомлень і документів. Положення набувають особливого значення з огляду на транскордонний характер міграційних процесів і необхідність обробки персональних даних у межах міграційних реєстрів та адміністративних процедур.

У міжнародно-правовому регулюванні захисту біженців відповідні гарантії мають більш опосередкований характер. Зокрема, Женевська конвенція про статус біженців 1951 року [36] прямо не формулює права на приватність, однак у практиці держав і міжнародних організацій сформувалися стандарти конфіденційності інформації про біженців, включаючи ідентифікаційні дані, матеріали особових справ та інші відомості, що підлягають належному захисту під час здійснення процедур надання міжнародного захисту.

Паралельно з розвитком універсальних міжнародно-правових стандартів відбувалося формування регіональних механізмів забезпечення права на повагу до приватного життя, які надалі відіграли важливу роль у деталізації та практичному застосуванні відповідних гарантій.

Найбільш інституційно розвинуту систему захисту права на приватність сформовано у межах РЄ. Важливим нормативним актом стала Європейська конвенція з прав людини [46], відповідно до статті 8 якої гарантується право на повагу до приватного і сімейного життя, житла та кореспонденції. Частина друга статті 8 встановлює критерії допустимості втручання держави у реалізацію цього права, зокрема вимоги законності, легітимної мети та необхідності у демократичному суспільстві.

Подальший розвиток змісту зазначеної норми був забезпечений практикою ЄСПЛ, який сформував підхід до динамічного тлумачення положень ЄКПЛ та суттєво розширив зміст поняття «*приватне життя*». Зокрема, до нього було включено інформаційний аспект приватності, що охоплює питання обробки персональних даних, використання електронних засобів комунікації та зберігання біометричної інформації.

У своїх рішеннях Суд також сформулював так званий триетапний тест допустимості втручання, відповідно до якого будь-яке втручання у приватне життя повинно бути «*передбаченим законом»,* переслідувати легітимну мету та бути «*необхідним у демократичному суспільстві*», тобто відповідати принципу пропорційності.

Подальша конкретизація зазначених стандартів у контексті мсового цифрового спостереження була здійснена у справі Big Brother watch and Others v. the United Kindom [27], в якій ЄСПЛ сформулював вимоги до «*якості закону*» в умовах використання технологій перехоплення електронних комунікацій, підкресливши необхідність наявності ефективних гарантій незалежного контролю та запобігання зловживаннями. Однак, зважаючи на актуальність відповідної проблематики та значний обсяг практику Суду, більш детальний аналіз зазначеної справи та пов’язаних правових підходів було здійснено у межах апробації результатів дослідження в тезах «Захист права на приватність у цифровому середовищі: аналіз практики ЄСПЛ» наукової конференції «Міжнародне та публічне право: перспективи та виклики» 2026 року [21].

У зв’язку зі стрімким розвитком інформаційних технологій особливого значення набуло прийняття у 1981 році Конвенція №108 про захист осіб у зв’язку з автоматизованою обробкою персональних даних [31], яка стала першим міжнародним договором у сфері інформаційної приватності. Відповідно до положень Конвенції закріплено принципи законності обробки даних, їх цільового використання, пропорційності, точності та безпеки. Слід окремо зазначити, що подальша модернізація зазначеного міжнародного інструменту була здійснена шляхом прийняття у 2018 році Протоколу CETS №223 про внесення змін до Конвенції №108 [62], у результаті чого оновлений договір отримав назву Конвенція 108+, що відобразило адаптацію міжнародних стандартів захисту персональних даних до умов цифрової трансформації та глобалізації інформаційних процесів. Станом на 2026 рік важливим залишається питання імплементації модернізованої Конвенції 108+ [31] державами-учасницями. Хоча Україна підписала Протокол у 2018 році, його ратифікація на національному рівні станом на сьогодні не завершена.

Подальший розвиток міжнародно-правових стандартів у сфері інформаційної приватності відбувся із прийняттям у 2001 році Конвенція про кіберзлочинність [33] Ради Європи, також відомої як Будапештська конвенція, яка встановила міжнародні механізми боротьби з кіберзлочинністю та водночас передбачила гарантії захисту прав людини під час здійснення електронного контролю й обробки цифрової інформації. Важливим етапом подальшого розвитку цього інструменту стало прийняття Другого додаткового протоколу 2022 року [69] щодо посилення співпраці та розкриття електронних доказів, який створив додаткові процесуальні гарантії та механізми доступу до даних із відповідними запобіжниками захисту прав людини.

В Американській конвенції з прав людини 1969 року [24], стаття 11 проголошує право кожної особи на повагу до честі та репутації, а також на захист від довільного чи незаконного втручання в її приватне життя, сім’ю, житло або кореспонденцію. Комісія та Суд міжамериканської системи захисту прав людини розвинули відповідну юриспруденцію щодо стеження, прослуховування та обробки персональних і телекомунікаційних даних, акцентуючи увагу на вимогах законності та пропорційності. На рівні політик Організація американських держав в 2015 ухвалила

Міжамериканські принципи захисту персональних даних [54], які стали актом «*м'якого права*» для зближення національних підходів до регулювання.

В Африці – Африканська хартія прав людини і народів 1981 року [22] не містить окремої прописаної норми права на приватність, проте у взаємозв'язку з гарантіями гідності, недискримінації та свободи особи це право виводиться із загальних положень Хартії. Спеціальним інструментом у цій сфері стала Конвенція Африканського Союзу про кібербезпеку та захист персональних даних 2014 [32], яка встановлює правові рамки для створення органів нагляду, визначає права суб'єктів даних і регулює транскордонну передачу інформації.

В арабському регіоні Арабська хартія прав людини (переглянута у 2004 році) [22] гарантує повагу до приватного життя, честі та репутації, тоді як у практиці держав посилюється галузеве регулювання захисту персональних даних.

У праві Європейського Союзу право на приватність і захист персональних даних набули конституційного статусу через Хартію основних прав [30], яка закріпила дуалістичну модель правового регулювання приватності. Зокрема, стаття 7 гарантує право на повагу до приватного і сімейного життя, а стаття 8 встановлює автономне право на захист персональних даних.

Істотним етапом розвитку європейського законодавства у сфері інформаційної приватності стало прийняття у 1995 році Директива 95/46/ЄС про захист персональних даних [43], яка заклала базові принципи регулювання обробки персональної інформації в межах Європейського Союзу та стала основою для подальшої уніфікації законодавства держав-членів та стала фундаментом для Загального регламенту про захист даних 2016 року [64], який сформував комплексну модель регулювання обробки персональних даних у цифровому середовищі. Зокрема, стаття 5 Регламенту визначає основні принципи обробки персональних даних, а стаття 25 закріплює концепції «*privacy by design*» та «*privacy by default*», що передбачають інтеграцію механізмів захисту приватності у процес розроблення інформаційних технологій.

Отож, історична еволюція права на приватність у міжнародному праві демонструє поступовий перехід від загальних декларативних положень до складної

системи універсальних і регіональних нормативних стандартів, що регулюють як традиційні аспекти недоторканності особистого життя, так і сучасні інформаційні процеси. Універсальні міжнародні акти сформували базовий рівень гарантій поваги до приватного життя, тоді як регіональні правові системи забезпечили подальшу деталізацію та розвиток відповідних механізмів правового захисту.

Однією з новітніх тенденцій розвитку міжнародно-правового регулювання стало поступове формування права на захист персональних даних як відносно автономного елементу правового режиму приватності. У європейській правовій моделі чітко простежується розмежування між правом на повагу до приватного життя як сферою особистої автономії та правом на інформаційне самовизначення, що передбачає контроль особи над обробкою її персональних даних. Таке розмежування сприяло посиленню процесуальних гарантій захисту даних, включаючи вимоги щодо прозорості обробки інформації, оцінки впливу на захист даних, діяльності незалежних наглядових органів, а також механізмів контролю за транскордонною передачею інформації.

Водночас цифровізація суспільних відносин поставила перед міжнародним правом низку нових викликів. Поширення технологій масового нагляду, біометричної ідентифікації, систем відеоспостереження, інтернету речей, великих даних та штучного інтелекту істотно трансформує межі між приватною та публічною сферами. У таких умовах дедалі складніше визначити баланс між інтересами державної безпеки, економічного розвитку, свободи вираження поглядів та необхідністю гарантування права людини на приватність.

Реакцією міжнародної спільноти на ці виклики стало посилення принципів законності, необхідності та пропорційності втручання у приватне життя, а також розвиток додаткових гарантій у сфері обробки персональних даних. Серед них — принцип мінімізації даних, вимоги щодо безпеки та конфіденційності інформації, запровадження технічних і організаційних заходів захисту даних «*за задумом і за замовчуванням*», а також посилення ролі незалежних наглядових органів і міжнародної регуляторної співпраці. Особливе значення набувають також механізми

правової взаємодії держав у сфері транскордонних потоків даних та розслідування порушень, пов’язаних із цифровими технологіями.

Важливим аспектом сучасного розвитку є також формування більш збалансованого підходу до співвідношення права на приватність з іншими фундаментальними цінностями, зокрема національною безпекою, свободою вираження поглядів, науковими дослідженнями та економічними інтересами. У цьому контексті міжнародні органи з прав людини наголошують на необхідності забезпечення чітких і передбачуваних правових рамок для здійснення заходів нагляду, наявності ефективного судового та інституційного контролю, а також доступності засобів правового захисту для осіб, права яких можуть бути порушені.

Отже, сучасна міжнародно-правова система захисту приватності формується як багаторівнева структура, що поєднує універсальні стандарти, регіональні механізми та спеціалізовані норми, спрямовані на регулювання цифрового середовища. У центрі цієї системи залишається принцип людської гідності та автономії особи, які визначають фундаментальне значення приватності для забезпечення свободи, самовираження, недискримінації та демократичного врядування.

У зв’язку з цим особливого значення набуває розвиток міжнародних політичних і рекомендаційних актів, у яких держави та міжнародні організації реагують на нові виклики цифрової епохи. Зокрема, у резолюціях міжнародних органів з прав людини дедалі частіше порушуються питання масового нагляду, цифрових прав людини та необхідності формування національних правових механізмів захисту приватності в умовах розвитку інформаційних технологій.

1.3. Вплив сучасних кіберзагроз та технологій штучного інтелекту на реалізацію права на цифрову приватність: міжнародно-правовий вимір.

Сучасний етап розвитку інформаційного суспільства характеризується глибокою цифровою трансформацією суспільних відносин, що істотно впливає на механізми реалізації фундаментальних прав і свобод людини. Одним із прав, яке зазнає найбільш відчутних змін унаслідок розвитку інформаційних технологій, є право на приватність. Якщо на попередніх етапах розвитку міжнародного права основна увага приділялася захисту недоторканності житла, сімейного життя та

таємниці кореспонденції, то в умовах цифровізації суспільства ключового значення набуває забезпечення захисту персональних даних та інформаційної автономії особи у цифровому середовищі.

У сучасній правовій доктрині дедалі частіше використовується поняття цифрової приватності, яке відображає специфіку реалізації права на приватність у середовищі глобальних інформаційних мереж. У загальному розумінні приватність пов'язується з правом особи зберігати свої особисті справи та інформацію поза стороннім втручанням. Згідно з підходом, що відображений у Cambridge Dictionary, поняття «*privacy»* пов'язується з правом людини зберігати свої особисті справи та інформацію конфіденційними, тоді як «*data»* розуміються як інформація або відомості, що збираються та використовуються для подальшого аналізу або прийняття рішень. Поєднання цих категорій у сучасному правовому дискурсі формує концепцію *«data privacy»,* яка охоплює правові питання, пов'язані зі збиранням, обробкою, зберіганням та поширенням інформації, що дозволяє ідентифікувати особу [16].

Зважаючи на це, цифрова приватність розглядається як можливість особи здійснювати контроль над збором, обробкою, використанням та поширенням даних про себе в електронному середовищі, включаючи персональні дані, дані електронних комунікацій, поведінкову інформацію та інші цифрові сліди діяльності людини. Таким чином, право на цифрову приватність охоплює не лише традиційні аспекти особистого життя, а й ширший комплекс суспільних відносин, пов'язаних із функціонуванням інформаційних систем та обробкою значних масивів даних.

Формування концепції цифрової приватності безпосередньо пов'язане з розвитком глобальної мережевої інфраструктури, що забезпечує швидке поширення інформації та інтеграцію цифрових технологій у всі сфери суспільного життя. У сучасному світі значна частина комунікації, економічної діяльності та соціальної взаємодії відбувається через цифрові платформи та інформаційні системи. У результаті обсяг відомостей про особу, що створюється, накопичується та обробляється в електронному середовищі, постійно зростає. Така ситуація зумовлює виникнення нових ризиків для приватності, оскільки значні масиви персональних

даних можуть використовуватися як державними органами, так і приватними суб'єктами для різних цілей.

Одним із ключових чинників, що впливають на реалізацію права на цифрову приватність, є поширення сучасних кіберзагроз. У міжнародному правовому та технічному дискурсі кіберзагрози розглядаються як сукупність потенційних або реальних дій, спрямованих на порушення конфіденційності, цілісності або доступності даних та інформаційних систем. До таких загроз належать несанкціонований доступ до комп'ютерних систем, незаконне перехоплення електронних комунікацій, викрадення персональних даних, використання шкідливого програмного забезпечення, кібершпигунство, а також інші форми втручання у функціонування цифрової інфраструктури.

Поширення кіберзагроз безпосередньо пов'язане зі зростанням залежності сучасних суспільств від цифрових технологій. Інформаційні системи використовуються для зберігання значних обсягів даних, включаючи персональну інформацію користувачів, фінансові дані, медичні записи та інші конфіденційні відомості. У разі порушення безпеки таких систем існує ризик масового витоку інформації, що може мати серйозні наслідки для приватного життя людей.

Показовим прикладом ризиків для реалізації права на приватність у цифровому середовищі є скандал, пов'язаний із діяльністю компанії Cambridge Analytica та соціальної платформи Facebook, що набув широкого міжнародного розголосу у 2018 році. Випадок привернув значну увагу урядів, регуляторних органів та наукової спільноти до проблеми неконтрольованої обробки персональних даних у межах великих цифрових платформ [53].

Фактичні обставини інциденту були пов'язані з використанням технічної інфраструктури платформи Facebook, яка дозволяла стороннім розробникам отримувати доступ до певних категорій інформації користувачів через програмний інтерфейс додатків (Application Programming Interface, API). Функціональні можливості відповідного інтерфейсу передбачали доступ до даних користувачів, які взаємодіяли із зовнішніми додатками, а також до окремих відомостей про їхні соціальні контакти та інтереси, що відображалися у профілях соціальної мережі.

У результаті використання таких технічних можливостей відбулося масштабне збирання персональних даних користувачів соціальної мережі. Зібрані дані включали відомості про інтереси, поведінкові характеристики та соціальні зв'язки користувачів. Подальша аналітична обробка такої інформації дозволила сформувати детальні цифрові профілі осіб, що використовувалися для здійснення так званого політичного мікротаргетингу — адресного поширення політичних повідомлень з урахуванням індивідуальних характеристик і поведінкових моделей окремих груп виборців.

За наявними оцінками, обсяг зібраної інформації охоплював дані приблизно 50 мільйонів профілів користувачів соціальної мережі. Інформація про використання персональних даних у зазначених цілях стала предметом широкого суспільного обговорення після оприлюднення журналістських розслідувань у 2018 році, зокрема у виданнях The Guardian та The New York Times. Публікація відповідних матеріалів спричинила численні парламентські слухання та регуляторні перевірки у різних державах, зокрема у США та Великій Британії [53].

З правової точки зору зазначена ситуація порушила питання дотримання фундаментальних принципів обробки персональних даних. Передусім виникли сумніви щодо забезпечення належного рівня прозорості обробки інформації, а також щодо дотримання вимог законності використання персональних даних та обмеження цілей їх обробки. Користувачі соціальної мережі фактично не були належним чином проінформовані про можливість передачі їхніх персональних даних третім особам та про подальше використання даних для проведення політичного аналізу і таргетування.

Офіційну правову оцінку відповідних обставин надало національне регуляторне відомство у сфері захисту персональних даних Сполученого Королівства — Information Commissioner's Office. За результатами проведеного розслідування було встановлено порушення вимог законодавства про захист персональних даних, передбачених Data Protection Act 1998 [39]. Регулятор дійшов висновку, що платформа Facebook не забезпечила належного рівня прозорості щодо використання персональних даних користувачів та не здійснила достатніх заходів для запобігання

їх неправомірному використанню третіми особами. Згідно з цього, на компанію було накладено адміністративний штраф у розмірі 500 000 фунтів стерлінгів, що становило максимальний розмір санкції, передбачений чинним на той момент законодавством.

Інцидент, пов’язаний із діяльністю Cambridge Analytica, продемонстрував системні ризики, що виникають унаслідок масштабної комерційної обробки персональних даних у цифровому середовищі. Події навколо використання даних користувачів соціальних мереж стали важливим фактором подальшого розвитку правового регулювання у сфері захисту персональних даних, а також посилили міжнародну увагу до необхідності встановлення ефективних гарантій забезпечення цифрової приватності [53].

Крім того, кіберзагрози можуть проявлятися у формі незаконного стеження або збору інформації про діяльність користувачів у мережі Інтернет. Сучасні технології дозволяють відстежувати поведінку користувачів, їхні інтереси, місцезнаходження та інші аспекти цифрової активності. Інформація може використовуватися для комерційних цілей, зокрема у сфері цифрової реклами, або для здійснення державного контролю та нагляду.

Ілюстрацією ризиків, пов’язаних із масштабним електронним спостереженням, є практика масового перехоплення електронних комунікацій, що стала предметом розгляду у справі Meta Platforms Inc. v. Bundeskartellamt [61], рішення у якій було ухвалене Судом Європейського Союзу (далі – Суд ЄС, Суд) 4 липня 2023 року. Спір виник у зв’язку з рішенням Федерального відомства з питань конкуренції Німеччини, яке встановило, що компанія Meta здійснювала масштабний збір та об’єднання персональних даних користувачів соціальної мережі Facebook не лише з власної платформи, але й з інших сервісів екосистеми компанії (зокрема Instagram та WhatsApp), а також із сторонніх вебсайтів і мобільних додатків, на яких були інтегровані інструменти Facebook.

Практика дозволяла компанії формувати детальні цифрові профілі користувачів шляхом аналізу їхньої поведінки у мережі Інтернет, включаючи відвідування сторонніх вебресурсів, взаємодію з контентом та інші елементи цифрової активності.

На підставі цього здійснювалося персоналізоване таргетування реклами та інші форми комерційного використання даних.

Оцінюючи правомірність таких дій, суд застосував положення GDPR, зокрема статті 6 та 9 Регламенту. Суд встановив, що обробка персональних даних повинна ґрунтуватися на одній із законних підстав, визначених у статті 6 GDPR [64]. Разом з тим у цій справі компанія не змогла довести наявність належної правової підстави для широкомасштабного збору та об'єднання даних користувачів.

Суд ЄС також звернув увагу на те, що частина зібраної інформації могла опосередковано розкривати так звані чутливі персональні дані, зокрема політичні погляди, релігійні переконання або сексуальну орієнтацію, що підпадає під спеціальний режим захисту відповідно до статті 9 GDPR [64]. У таких випадках обробка даних допускається лише за наявності чітко визначених винятків або за умови отримання явної та недвозначної згоди суб'єкта даних.

Крім того, було підкреслено, що згода користувача повинна бути добровільною, конкретною, поінформованою та недвозначною. Якщо доступ до основної послуги обумовлюється необхідністю погодитися на масштабну обробку персональних даних, така згода не може вважатися добровільною.

У результаті Суд дійшов висновку, що практика збору та об'єднання персональних даних користувачів без належної правової підстави може розглядатися як порушення вимог GDPR. Водночас було зазначено, що порушення законодавства про захист персональних даних може слугувати важливим фактором при встановленні зловживання домінуючим становищем на ринку відповідно до норм конкурентного права Європейського Союзу.

Поряд із поширенням кіберзагроз значний вплив на трансформацію механізмів реалізації права на приватність здійснює розвиток технологій штучного інтелекту. Під ШІ у сучасному правовому та технологічному дискурсі розуміють системи, здатні виконувати завдання, які традиційно потребують інтелектуальної діяльності людини. До таких завдань належать аналіз даних, розпізнавання образів, прогнозування поведінкових моделей, автоматизоване прийняття рішень та інші складні аналітичні операції.

Технології ШІ активно застосовуються у різних сферах суспільного життя, включаючи електронну комерцію, фінансові послуги, медицину, державне управління та системи безпеки. Водночас їх використання передбачає обробку значних обсягів інформації, що часто включає персональні дані користувачів. Алгоритми машинного навчання потребують великих масивів даних для формування моделей прогнозування, що зумовлює інтенсивне накопичення інформації про поведінку користувачів, їхні уподобання, соціальні зв'язки та інші аспекти приватного життя.

З огляду на контекст, особливу увагу привертає проблема автоматизованого профілювання. Профілювання передбачає використання алгоритмів для аналізу персональних даних з метою оцінювання певних характеристик особи, зокрема її економічного становища, інтересів, поведінки або ймовірних майбутніх дій. Хоча такі технології можуть використовуватися для підвищення ефективності послуг або персоналізації контенту, вони водночас створюють ризики для приватності, оскільки дозволяють формувати детальні цифрові профілі користувачів.

Додатково важливим аспектом використання ШІ є застосування технологій біометричної ідентифікації. Біометричні системи використовують фізичні або поведінкові характеристики людини — такі як відбитки пальців, розпізнавання обличчя, голос або структура райдужної оболонки ока — для встановлення її особи. Використання таких технологій широко поширене у сфері безпеки, прикордонного контролю та доступу до цифрових сервісів. Водночас обробка біометричних даних викликає серйозні занепокоєння щодо захисту приватності, оскільки такі дані є унікальними та незмінними характеристиками людини.

Водночас новітнім етапом розвитку міжнародно-правового регулювання у сфері цифрової приватності стало прийняття у 2024 році Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію та верховенство права [37]. Зазначений міжнародний інструмент засвідчує поступовий перехід від регулювання, заснованого переважно на актах «*м'якого права*», що містять етичні принципи та рекомендаційні стандарти, до формування юридично обов'язкових норм у сфері використання технологій штучного інтелекту. Конвенція закріплює обов'язок держав

забезпечувати відповідність застосування систем ШІ вимогам захисту прав людини, зокрема права на повагу до приватного життя, а також передбачає створення механізмів оцінки ризиків, належного контролю та підзвітності. З огляду на це, можна констатувати становлення якісно нового етапу міжнародно-правового регулювання, маєш якого базується інституціоналізація жорстких регуляторних підходів до цифрових технологій.

З метою кращої практичної демонстрації правових проблем, пов'язаних із застосуванням технологій ШІ, варто звернутися до справи R (Bridges) v Chief Constable of South Wales Police [63], розглянутої Апеляційним судом Англії та Уельсу.

Суть спору полягала у використанні поліцією Південного Уельсу системи автоматичного розпізнавання обличь (Automatic Facial Recognition Locate) під час проведення публічних заходів у місті Кардіфф. Зазначена технологія функціонувала шляхом встановлення камер відеоспостереження у громадських місцях, які у режимі реального часу здійснювали сканування облич осіб, що проходили перед камерою. Отримані зображення автоматично оброблялися алгоритмами, які формували біометричні шаблони облич та порівнювали їх із даними так званих «списків спостереження», що містили інформацію про осіб, які перебували у розшуку або могли становити інтерес для поліції.

Позивач, Едвард Бріджес, оскаржив законність використання технології, стверджуючи, що автоматизоване сканування облич великої кількості осіб у публічному просторі призводить до обробки їхніх біометричних даних без згоди та без належних правових гарантій. На його думку, така практика становить втручання у право на приватне життя, гарантоване статтею 8 ЄКПЛ, а також порушує положення національного законодавства про захист персональних даних, зосібна вимоги Data Protection Act 2018 року [40] щодо законності обробки персональних даних та обов'язку проведення попередньої оцінки впливу на захист даних (Data Protection Impact Assessment) у випадках застосування нових технологій обробки інформації.

Розглядаючи справу, суд детально проаналізував особливості функціонування системи автоматичного розпізнавання облич. Було встановлено, що технологія дозволяє здійснювати масове збирання та обробку біометричних даних осіб, які

перебувають у зоні дії камер відеоспостереження, незалежно від того, чи є вони підозрюваними у вчиненні правопорушень. Хоча система зберігала дані лише у випадку виявлення збігу із «*списком спостереження*», сам факт автоматизованого сканування облич великої кількості громадян становив втручання у їхнє приватне життя.

Апеляційний суд дійшов висновку, що застосування технології автоматичного розпізнавання облич становить втручання у право на повагу до приватного життя відповідно до статті 8 ЄКПЛ [46]. Водночас Суд встановив, що нормативна база, яка регулювала використання цієї технології, не відповідала вимогам принципу законності. Зокрема, національне законодавство не містило достатньо чітких правил щодо критеріїв включення осіб до «списків спостереження», а також щодо визначення місць та обставин, у яких може застосовуватися така технологія. У результаті значний обсяг дискреційних повноважень залишався на розсуд правоохоронних органів.

Крім того, суд звернув увагу на те, що використання системи автоматичного розпізнавання облич пов’язане з ризиком дискримінаційних наслідків, оскільки алгоритми можуть демонструвати різний рівень точності щодо представників різних расових або гендерних груп. Відсутність належної оцінки таких ризиків також була визнана порушенням обов’язків державних органів у сфері захисту персональних даних.

З огляду на наведені обставини Апеляційний суд дійшов висновку, що використання поліцією системи автоматичного розпізнавання облич не відповідало вимогам статті 8 ЄКПЛ [46] та нормам законодавства про захист персональних даних.

Зазначене рішення має важливе значення для формування правових підходів до використання технологій ШІ у сфері публічної безпеки. Воно демонструє, що застосування систем біометричної ідентифікації повинно супроводжуватися чітким нормативним регулюванням, прозорими процедурами обробки персональних даних та ефективними гарантіями захисту права на приватність.

Вищезгадані процеси свідчать про те, що сучасний етап розвитку інформаційного суспільства супроводжується істотною трансформацією умов

реалізації права на приватність. Поширення кіберзагроз, масштабне накопичення та обробка персональних даних у цифровому середовищі, а також активне використання технологій штучного інтелекту створюють нові ризики для інформаційної автономії особи.

Як демонструє сучасна судова практика, використання цифрових технологій може призводити до масштабного збору та аналізу інформації про поведінку користувачів, формування детальних цифрових профілів осіб, а також до застосування систем автоматизованого спостереження, зокрема технологій біометричної ідентифікації. Такі тенденції істотно розширюють можливості як державних органів, так і приватних суб'єктів щодо обробки персональних даних, що, у свою чергу, підвищує ризики порушення права на повагу до приватного життя.

В контексті особливого значення набуває формування ефективних правових механізмів, спрямованих на забезпечення належного балансу між розвитком цифрових технологій та захистом фундаментальних прав людини. Міжнародне право поступово виробляє підходи до регулювання обробки персональних даних, використання алгоритмічних систем та застосування технологій штучного інтелекту, однак подальший розвиток таких механізмів залишається важливим завданням сучасної правової системи.

Аналізуючи попереднє, особливої уваги потребує аналіз міжнародно-правових стандартів та інституційних механізмів захисту цифрової приватності, що формуються у межах діяльності міжнародних організацій та інтеграційних об'єднань, оскільки формування ефективної системи міжнародно-правових гарантій у даній сфері є необхідною передумовою забезпечення балансу між розвитком інноваційних технологій та захистом фундаментальних прав людини у XXI столітті.

РОЗДІЛ 2
МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ТА МЕХАНІЗМИ ЗАХИСТУ ЦИФРОВОЇ ПРИВАТНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ ПРАВ ЛЮДИНИ ТА СУЧАСНИХ КІБЕРЗАГРОЗ

2.1. Універсальні та регіональні міжнародно-правові стандарти захисту цифрової приватності та персональних даних в умовах сучасних кіберзагроз.

Цифрова приватність у сучасному міжнародному праві постає не лише як продовження класичного права на недоторканність приватного життя, але як індикатор глибинної трансформації самих засад міжнародно-правового регулювання. Йдеться не просто про адаптацію вже існуючих прав людини до нових технологічних умов, а про зміну парадигми, в межах якої міжнародне право дедалі частіше покликане регулювати не статичні міждержавні відносини, а динамічні транснаціональні процеси, що відбуваються у віртуальному просторі.

Поява глобального кіберпростору, який не підпорядковується класичним принципам територіальності, юрисдикційної замкненості та суверенного контролю, поставила під сумнів ефективність традиційних механізмів захисту прав людини, сформованих у XX столітті, та актуалізувала питання про межі нормативної спроможності міжнародного права в умовах цифрової глобалізації.

Ключового значення набуває феномен сучасних кіберзагроз, які безпосередньо впливають на реалізацію права на цифрову приватність та захисту персональних даних. На відміну від класичних форм втручання у приватне життя, кіберзагрози характеризуються системністю, масштабністю та потенціалом для тривалого й прихованого впливу на особу. До таких загроз належать, зокрема, масове електронне спостереження, перехоплення цифрових комунікацій, несанкціонований доступ до баз персональних даних, зломи інформаційних систем, витоки конфіденційної інформації, а також використання алгоритмічних технологій для профілювання, прогнозування поведінки та автоматизованого ухвалення рішень. Спільною ознакою цих явищ є те, що вони створюють не поодинокі порушення, а структурну загрозу праву на приватність як такому.

Транснаціональний характер більшості кіберзагроз зумовлює необхідність їх регулювання на універсальному міжнародно-правовому рівні. Масове цифрове спостереження та транскордонна обробка персональних даних не обмежуються кордонами однієї держави, а отже потребують загальних стандартів допустимого втручання, заснованих на праві прав людини. Саме універсальні міжнародні норми покликані закріпити мінімальні гарантії цифрової приватності, що мають застосовуватися незалежно від технічних засобів і безпекових контекстів. Водночас універсальний рівень відіграє роль нормативного фундаменту, який обмежує можливість держав виправдовувати непропорційні цифрові втручання міркуваннями суверенітету або національної безпеки.

Водночас, специфіка сучасних кіберзагроз обумовлює зростаюче значення регіональних міжнародно-правових механізмів контролю. Саме на регіональному рівні стає можливим формування більш деталізованих стандартів, адаптованих до конкретних правових і технологічних реалій. Європейський регіональний підхід, зосібна, виходить із презумпції потенційної небезпеки цифрових технологій для прав людини і прагне встановити превентивні гарантії проти системних порушень приватності. Регіональні механізми дозволяють не лише конкретизувати універсальні норми, а й забезпечити ефективний нагляд за їх дотриманням через судові та квазісудові інститути.

Особливістю цифрової приватності є те, що вона функціонує в середовищі, де кордони між публічним і приватним, державним і недержавним, внутрішнім і міжнародним є структурно розмитими. Обробка персональних даних здійснюється одночасно у багатьох юрисдикціях, із залученням державних органів, транснаціональних корпорацій, хмарних сервісів алгоритмічних систем, що ускладнює ідентифікацію суб’єкта відповідальності та застосовного права. За цих умов захист персональних даних і цифрової приватності дедалі частіше опиняється на перетині трьох нормативних площин: міжнародного права прав людини, міжнародної безпеки та економічного суверенітету держав, кожна з яких висуває власні, нерідко конкуруючі вимоги.

Універсальні міжнародно-правові стандарти захисту приватності сформувалися як реакція на історичний досвід тоталітаризму та масових порушень прав людини у XX столітті. Загальна декларація прав людини [75] та Міжнародний пакт про громадянські і політичні права [56] виходили з презумпції, що головною загрозою приватності є держава, яка здійснює свавільне втручання у сферу особистого життя. Саме у той час зазначені акти закріплювали приватність у формі негативного суб'єктивного права, спрямованого на обмеження владних повноважень і забезпечення простору недоторканної автономії особи. Такий підхід відображав історичний контекст свого часу, у якому контроль над інформацією був здебільшого монополізований державними структурами та інституціями.

У цифрову епоху ця правова модель виявила свої концептуальні вади, оскільки значна частина збору, зберігання та аналізу персональних даних здійснюється не державами, а приватними суб'єктами, чия діяльність має транснаціональний характер і часто виходить за межі ефективного міжнародного або навіть національного контролю. Міжнародне право прав людини, збудоване навколо вертикальних відносин «*держава — індивід*», виявилося недостатньо підготовленим до горизонтальних і мережевих форм впливу на цифрову автономію особи, що здійснюються через комерційні платформи та інформаційні екосистеми.

Універсальні стандарти, зокрема положення раніше згаданої статті 17 МПГПП [56], не містять спеціалізованих норм щодо збору, зберігання, передавання та автоматизованого аналізу персональних даних. Вони не розмежовують типи даних, не встановлюють вимог до технічної безпеки обробки інформації та не враховують специфіку алгоритмічного профілювання. У відповідності до універсального права на приватність не дає чітких відповідей на виклики, пов'язані з масовим цифровим спостереженням, зберіганням метаданих, використанням ШІ або проведенням кібероперацій у сфері національної безпеки.

Навіть концепція законності втручання, яка традиційно відіграє ключову роль у міжнародному праві прав людини, втрачає визначеність у кіберпросторі. Технічні процеси обробки даних є непрозорими для пересічного суб'єкта права, а сама особа позбавлена можливості ефективно передбачити наслідки використання своїх

цифрових слідів. За таких умов формальна наявність правової підстави для втручання не гарантує відповідності такого втручання вимогам необхідності та пропорційності. З огляду на наведені обставини, універсальні міжнародно-правові стандарти дедалі більше виконують функцію морально-правового орієнтира, ніж інструменту прямого регулювання цифрових відносин.

Концептуальна обмеженість універсального підходу до захисту приватності в умовах цифрової епохи отримала часткове відображення у діяльності Організації Об'єднаних Націй, зокрема у процесі формування підходів до захисту права на приватність у цифровому середовищі. Резолюції Генеральної Асамблеї акцентують увагу на небезпеці масового електронного спостереження та неконтрольованої обробки персональних даних, визначаючи, що такі практики можуть мати *«chilling effect»* на реалізацію інших прав і свобод. У доктринальному розумінні стримувальний ефект означає не пряме обмеження прав, а їх опосередковану деформацію, коли сама наявність потенційного контролю або збору інформації змінює поведінку особи [28]. Усвідомлюючи можливість фіксації та подальшого використання своїх дій чи висловлювань, індивід схильний до самообмеження, що проявляється у звуженні простору реалізації фундаментальних свобод.

За таких умов втручання у приватність трансформується з індивідуального акту порушення у фактор, який системно впливає на функціонування демократичних інститутів, зокрема через обмеження свободи вираження поглядів і публічної участі. Водночас документи не трансформують структуру міжнародних зобов'язань держав і не створюють нових юридично обов'язкових механізмів відповідальності. Фактично йдеться про формування *soft law*, що фіксує політичний консенсус, але не забезпечує ефективного стримування кіберзагроз. У світлі наведеного аналізу цифрова приватність залишається сферою, де універсальне міжнародне право істотно відстає від технологічної реальності.

Вагомим елементом універсального міжнародно-правового механізму захисту цифрової приватності є мандат Спеціального доповідача ООН з права на приватність [58], запроваджений Радою ООН з прав людини у 2015 році. Його створення стало реакцією міжнародної спільноти на усвідомлення того, що традиційні інструменти

контролю за дотриманням права на приватність виявляються недостатніми в умовах розвитку цифрових технологій, масового електронного спостереження та транснаціональної обробки персональних даних.

На відміну від класичних контрольних механізмів, орієнтованих переважно на індивідуальні скарги або ретроспективну оцінку порушень, мандат Спеціального доповідача має превентивно-аналітичний характер. Його діяльність спрямована не лише на фіксацію окремих порушень, а й на виявлення системних загроз приватності, пов'язаних із використанням цифрових технологій, зокрема алгоритмічних систем, біометричних інструментів та технологій масового спостереження.

У своїх тематичних доповідях Спеціальний доповідач послідовно наголошує, що втручання у приватне життя в цифрову епоху має якісно інший характер порівняно з класичними формами порушень. Збір та аналіз великих масивів даних дозволяють формувати детальні цифрові профілі особи, здатні впливати на її поведінку, свободу самовираження та участь у публічному житті. У цьому сенсі приватність постає не лише як індивідуальне право, а як структурна передумова функціонування демократичного суспільства.

Особливе значення в межах мандата надається критеріям необхідності та пропорційності цифрових втручань. Спеціальний доповідач послідовно підкреслює, що посилання держав на міркування національної безпеки або технічну неминучість не можуть автоматично виправдовувати масове електронне спостереження, автоматизовану обробку персональних даних чи використання штучного інтелекту без належних правових гарантій. Навпаки, саме в умовах зростання кіберзагроз держава зобов'язана забезпечити чітке нормативне регулювання, ефективний нагляд та реальні механізми підзвітності.

Водночас діяльність Спеціального доповідача виявляє і концептуальні обмеження універсального міжнародного рівня. Його рекомендації та доповіді, хоча й формують важливі орієнтири розвитку стандартів права на приватність, не мають юридично обов'язкової сили та не супроводжуються ефективними санкційними механізмами. Враховуючи даний контекст, мандат виконує радше функцію

нормативного орієнтира та інтелектуального каталізатора, ніж інструменту безпосереднього регулювання цифрових практик.

З огляду на зазначене, мандат Спеціального доповідача ООН з права на приватність відіграє важливу роль у формуванні глобального дискурсу щодо цифрової приватності, водночас підкреслюючи необхідність поєднання універсальних стандартів із більш деталізованими та дієвими регіональними механізмами захисту, здатними ефективно реагувати на виклики цифрової епохи.

Регіональні міжнародно-правові стандарти демонструють принципово інший підхід, орієнтований не лише на декларацію прав, а й на управління ризиками цифрової епохи. Європейська модель захисту персональних даних сформувалася під впливом історичної недовіри до неконтрольованого державного та корпоративного накопичення інформації і ґрунтується на ідеї, що персональні дані є проявом особистості, а не нейтральним економічним ресурсом. Саме в межах європейського правового простору персональні дані були вперше концептуалізовані як об’єкт самостійного правового режиму, який виходить за межі класичного розуміння приватного життя.

ЄСПЛ, тлумачачи статтю 8 ЄКПЛ [46], поступово розширив її зміст до охоплення не лише втручання в інтимну сферу особи, але й будь-якого системного збирання, зберігання чи використання інформації, пов’язаної з нею. Регіональний підхід принципово відрізняється від універсального тим, що виходить із презумпції потенційної небезпеки цифрових технологій для прав людини і вимагає наявності інституційних та процедурних запобіжників навіть за відсутності доведеного зловживання.

Подальший розвиток регіональних стандартів у праві Європейського Союзу засвідчив перехід від правозахисної логіки до логіки регулювання цифрових процесів. Загальний регламент про захист даних [64] не лише гарантує суб’єктивні права, але й покладає системні обов’язки на контролерів і процесорів даних, встановлюючи вимоги до архітектури інформаційних систем, принципів обробки інформації та внутрішнього управління ризиками. Такий підхід свідчить про спробу

міжнародного та наднаціонального права впливати не лише на правові, але й на технічні умови існування цифрової приватності.

Разом із тим наукова критика регіональних стандартів концентрується на проблемі їхньої реальної ефективності в умовах зростаючих кіберзагроз. Попри нормативну деталізацію, право часто реагує на технологічні зміни із запізненням, тоді як інформаційна влада дедалі більше концентрується на рівні глобальних цифрових інфраструктур. Формалізовані процедури відповідності не завжди здатні змінити фундаментальний дисбаланс між суб'єктом персональних даних і операторами (контролерами) обробки, що створює ризик перетворення навіть найбільш розвинених регіональних режимів на механізм легітимації цифрових практик замість їх реального обмеження.

Аналіз викладеного свідчить про те, що універсальні та регіональні міжнародно-правові стандарти захисту цифрової приватності відображають різні рівні адаптації міжнародного права до викликів цифрової епохи. Універсальні норми формують базовий нормативний каркас, закріплюючи загальні межі допустимого втручання у приватне життя, однак їх абстрактність та відсутність спеціалізованих механізмів обмежують ефективність у протидії сучасним кіберзагрозам. Натомість регіональні правові системи, передусім європейська, забезпечують більш високий рівень деталізації та інституціоналізації відповідних стандартів, поєднуючи нормативне регулювання з механізмами контролю за його дотриманням.

Водночас навіть у межах розвинених регіональних моделей ключове значення набуває не лише формальне закріплення правових гарантій, але й їх практичне тлумачення та застосування у конкретних правовідносинах. Власне у площині правозастосовної діяльності відбувається наповнення абстрактних норм реальним змістом, зокрема через формування підходів до оцінки допустимості втручання у цифрову приватність, балансування між безпековими інтересами та правами людини, а також адаптації класичних правових критеріїв до новітніх технологічних реалій.

Враховуючи зазначене, особливого значення набуває практика ЄСПЛ яка відіграє ключову роль у конкретизації змісту права на повагу до приватного життя в

умовах цифровізації та формуванні стандартів захисту персональних даних у сучасному правовому просторі.

2.2. Практика Європейського суду з прав людини щодо захисту цифрової приватності та персональних даних.

Цифрова епоха зумовила докорінно трансформацію способів реалізації, обмеження та захисту прав людини. Масове впровадження інформаційно-комунікаційних технологій, розвиток цифрових платформ, алгоритмічна управління та біометричних систем істотно розширили можливості держави та приватних суб'єктів щодо доступу до персональних інформації. Водночас такі процеси супроводжується зростанням кіберзагроз — як у вигляді несанкціонованого доступу до даних, так і у формі легалізовано масово спостереження, що здійснюється під підкриттям публічних інтересів. Площина права на повагу до приватного життя набуває якісного нового змісту, ідеться вже не лише про захист фізичної або інтимної сфери особи, про гарантування її цифрової автономії, тобто можливості контролювати обіг, використання та зберігання інформації, яка формує цифровий портрет особи. За відсутності спеціалізованих норм у межах ЄКПЛ практика ЄСПЛ виступає основним нормативним орієнтиром, що сприяє адаптації класичних правових стандартів до викликів кіберпростору.

ЄСПЛ послідовно наголошує, що стаття 8 Конвенції [46] має автономне та еволюційний характер. Поняття «*приватного життя*» не обмежується сферою особистих або сімейних відносин, а охоплює також інформаційний вимір особистості, зокрема персональні та біометричні дані, цифрові комунікації, онлайн-поведінку та професійну діяльність.

Ключовим елементом аналізу є критерій *«втручання».* Суд визначає, що збирання, зберігання або систематизація персональних даних державними органами становить втручання незалежно від того, що відбулося подальше використання таких даних. Саме такий підхід дозволяє розглядати цифрові технології як потенційно небезпечні для приватності вже на стадії організаційно впровадження.

Заразом практика ЄСПЛ демонструє взаємозв'язок статті 8 з іншими положеннями ЄКПЛ. Зосібна, стаття 10 постає релевантною у контексті розповсюдження персональної інформації через цифрові медіа; стаття 11 — у випадках, коли цифрове спостереження створює стримувальний ефект для свободи зібрань; стаття 6 — коли цифрові дані стають

підставою для притягнення до юридичної відповідальності [46]. Така багатовимірність підкреслює системний вплив цифрових практик на всю архітектуру прав людини, що зумовлює доцільність звернення до аналізу релевантної практики ЄСПЛ.

Справу Gaughran v. the United Kingdom [48] було порушено у зв'язку з безстроковим зберіганням правоохоронними органами біометричних даних заявника, засудженого за правопорушення незначної тяжкості. Після його арешту за керування транспортним засобом у стані алкогольного сп'яніння поліція здійснила збирання його фотографії, відбитків пальців та ДНК-зразка. Попри те, що заявник визнав свою вину, був підданий штрафу та тимчасовому обмеженню права керування транспортними засобами, а сама судимість згодом була погашена, відповідні біометричні дані (зокрема ДНК-профіль, відбитки пальців і фотографії) продовжували зберігатися поліцією на невизначений строк.

Відповідно до національного правового регулювання, такі дані осіб, засуджених за злочини, підлягали автоматичному та безстроковому зберіганню незалежно від тяжкості правопорушення, подальшої поведінки особи чи наявності потреби у їх подальшому використанні. Національні суди, включаючи Верховний суд, відмовили заявникові у задоволенні позову, обґрунтовуючи це інтересами ефективності кримінального правосуддя.

Однак ЄСПЛ дійшов протилежного висновку, визнавши порушення статті 8 Конвенції. Суд погодився, що втручання було «*передбачене законом*» і переслідувало легітимну мету — запобігання злочинності, проте ключовим стало питання його відповідності критерію «*необхідності в демократичному суспільстві*». З огляду на це, Суд наголосив, що оцінка пропорційності повинна здійснюватися з урахуванням усієї системи зберігання даних, а не лише тривалості такого зберігання.

Особливого значення Суд надав тому, що національний режим фактично надавав державі максимально широкі повноваження щодо безстрокового зберігання біометричної інформації без належних запобіжників. Зокрема, зберігання здійснювалося без урахування тяжкості вчиненого правопорушення, без оцінки подальшої необхідності такого зберігання, а також за відсутності ефективного механізму перегляду або видалення даних. За таких умов було порушено справедливий баланс між публічними інтересами та правом особи на повагу до приватного життя, що зумовило визнання втручання непропорційним.

ЄСПЛ також підкреслив, що в умовах розвитку цифрових технологій навіть традиційні форми ідентифікації, такі як фотографії, набувають нового значення, оскільки можуть використовуватися у системах розпізнавання обличчя та інтегруватися в масштабні бази даних. У цьому рішенні вперше було прямо визнано, що саме збирання та зберігання фотографій становить втручання у право на приватність.

Водночас Суд звернув увагу на особливу чутливість ДНК-даних, які здатні розкривати не лише інформацію про саму особу, а й про її генетичні зв'язки з іншими людьми, що розширює потенційне коло втручання у приватне життя. Це, в свою чергу, означає, що зберігання та подальший аналіз таких даних може опосередковано впливати на приватність третіх осіб, зокрема шляхом встановлення сімейних зв'язків (наприклад, батьківства чи спорідненості), навіть без їхньої згоди або відома.

Крім того, Суд критично оцінив аргументацію держави щодо того, що розширення обсягів зберігання даних сприяє ефективнішій боротьбі зі злочинністю, зауваживши, що подібна логіка може призвести до надмірного та невиправданого накопичення інформації про все населення, що є несумісним із принципами демократичного суспільства [48].

У справі M.M. v. the United Kingdom [57] ЄСПЛ розглянув питання тривалого зберігання та подальшого розкриття правоохоронними органами інформації про застосування до заявниці заходу у вигляді «*caution*» (офіційного попередження), винесеного без відкриття кримінального провадження. Заявниця надала згоду на перевірку судимості у зв'язку з працевлаштуванням у сфері соціальної роботи, однак саме наявність відповідного запису в поліцейських базах даних стала підставою для відмови у прийнятті на роботу.

Особливістю цієї справи було те, що заявницю раніше було запевнено у тимчасовому характері зберігання відповідної інформації — строк її зберігання мав становити п'ять років. Проте внаслідок зміни політики правоохоронних органів дані почали зберігатися безстроково, зокрема у випадках, пов'язаних із правопорушеннями щодо дітей, незалежно від їх фактичної тяжкості чи наслідків. Попри численні звернення заявниці, інформація не була видалена, а натомість пропонувалося лише додати пояснювальну примітку до запису.

Національні органи влади визнали такі дії правомірними, обґрунтовуючи їх інтересами публічної безпеки та необхідністю захисту прав інших осіб. Водночас ЄСПЛ дійшов протилежного висновку, встановивши порушення статті 8 Конвенції [46]. Суд

підкреслив, що як зберігання персональних даних, так і їх подальше розкриття третім особам (зокрема потенційним роботодавцям) становлять втручання у право на повагу до приватного життя.

Ключовим у даній справі стало те, що відповідна інформація, навіть будучи формально публічною, з плином часу набуває ознак елементу приватного життя особи. Системне зберігання та доступність таких даних призводить до їх тривалого впливу на соціальний статус особи, зокрема у сфері працевлаштування, коли фактично формується її «*цифровий профіль*», який не зникає навіть після втрати правового значення відповідної події.

Суд також звернув увагу на відсутність чіткої законодавчої бази, яка б регулювала порядок збирання, зберігання та розкриття таких даних. На момент подій у Північній Ірландії відповідні процедури здійснювалися на основі загальних повноважень поліції та внутрішніх політик, що не забезпечувало належної визначеності та передбачуваності правового регулювання. Крім того, відсутні були ефективні механізми незалежного перегляду рішень про подальше зберігання чи розкриття інформації.

Особливо критичним Суд визнав те, що система не передбачала диференційованого підходу: не враховувалися ані характер правопорушення, ані час, що минув з моменту його вчинення, ані релевантність інформації для конкретної посади, на яку претендувала заявниця. Підхід фактично призводив до автоматизованого та невизначеного у часі обмеження професійних можливостей особи [57].

Підсумовуючи, ЄСПЛ дійшов висновку, що держава не забезпечила справедливого балансу між суспільним інтересом та правом заявниці на повагу до приватного життя. Відсутність належних правових гарантій, чітких строків зберігання даних і ефективних механізмів контролю призвела до непропорційного втручання у її права.

Окремо слід згадати справу Bărbulescu v. Romania [26] предметом розгляду стало питання допустимості моніторингу роботодавцем електронної комунікації працівника в умовах цифрового середовища. Заявник, який працював інженером з продажу, за вимогою роботодавця створив обліковий запис у службовому месенджері для виконання професійних обов’язків. Попри існування внутрішніх правил, що забороняли використання корпоративних ресурсів у приватних цілях, заявника було звільнено після того, як

роботодавець здійснив моніторинг його повідомлень і встановив факти особистого листування.

Національні суди підтримали позицію роботодавця, фактично виходячи з того, що службовий характер комунікації виключає або істотно обмежує сферу приватності працівника. Водночас Велика палата ЄСПЛ відкинула такий формальний підхід, наголосивши, що сам факт використання корпоративних засобів зв'язку не нівелює права особи на повагу до приватного життя та кореспонденції у розумінні статті 8 Конвенції [46].

Суд підтвердив широке тлумачення поняття «*приватного життя*», яке охоплює також професійну діяльність та комунікацію в робочому середовищі, включаючи електронне листування. Водночас він підкреслив, що у таких справах йдеться про позитивні зобов'язання держави забезпечити справедливий баланс між інтересами роботодавця та правами працівника. Хоча державам надається певна свобода розсуду у регулюванні питань контролю за працівниками, вона не є необмеженою та повинна реалізовуватися з дотриманням принципу пропорційності та наявності ефективних процесуальних гарантій.

Велика палата сформулювала низку критеріїв, які мають враховуватися при оцінці допустимості моніторингу: поінформованість працівника про можливість і характер контролю; обсяг і ступінь втручання (зокрема, відмінність між відстеженням метаданих і доступом до змісту повідомлень); наявність обґрунтованої мети такого втручання; можливість застосування менш інвазійних засобів; наслідки моніторингу для працівника; а також існування належних гарантій проти зловживань.

У конкретній справі Суд встановив, що хоча заявник був загально поінформований про можливість контролю, він не був належним чином повідомлений про його обсяг і характер, зокрема про можливість доступу роботодавця до змісту повідомлень. Крім того, національні суди не здійснили належної оцінки пропорційності втручання: не було встановлено чіткої мети моніторингу, не оцінено ступінь втручання у приватність, а також не розглянуто альтернативні, менш обмежувальні заходи.

Підсумовуючи, Велика палата встановила, що мало місце порушення статті 8 Конвенції [46], зазначивши, що національні органи не забезпечили справедливого балансу між конкуруючими інтересами, а отже, не гарантували належного захисту права заявника на приватне життя та кореспонденцію [26].

З урахуванням специфіки цифрової приватності необхідно також враховувати взаємозв'язок статті 8 ЄКПЛ зі статтею 10, яка гарантує свободу вираження поглядів [40]. У цифрову епоху реалізація даної свободи дедалі частіше відбувається під впливом алгоритмічних рішень, зокрема механізмів автоматизованої модерації контенту, ранжування інформації та персоналізованої реклами. Практика ЄСПЛ послідовно підкреслює, що використання технологічних засобів саме по собі не може слугувати підставою для зниження стандартів захисту прав, передбачених Конвенцією.

Особливого значення набувають справи, у яких поширення персональних даних здійснюється за допомогою цифрових платформ або автоматизованих сервісів. Суд виходить із того, що масове, структуроване та технологічно посилене поширення інформації істотно відрізняється від її традиційного оприлюднення, оскільки здатне значно підвищити інтенсивність втручання у приватне життя.

Показовим у цьому контексті є рішення у справі Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [68], де Суд розглядав питання масового поширення податкових даних фізичних осіб. Попри те, що відповідна інформація у Фінляндії формально була публічно доступною, її масштабна агрегація та розповсюдження через друковане видання і SMS-сервіс суттєво змінили характер доступу до неї. ЄСПЛ наголосив, що така форма обробки даних робить інформацію доступною у значно ширшому обсязі та в інший спосіб, ніж це передбачалося законодавцем, що створює додаткові ризики для приватності.

Водночас Суд визнав, що обмеження, встановлені національними органами щодо такого способу обробки та поширення даних, не порушили статтю 10 Конвенції. Він дійшов висновку, що втручання було передбачене законом, переслідувало легітимну мету захисту приватного життя платників податків та було необхідним у демократичному суспільстві. При цьому Суд підкреслив, що масове оприлюднення персональних даних не сприяло обговоренню питань суспільного інтересу, а отже не користувалося підвищеним рівнем захисту як форма свободи вираження поглядів.

У ширшому контексті ця справа відображає важливу тенденцію у практиці ЄСПЛ: навіть формально публічна інформація може підпадати під захист статті 8 Конвенції [23], якщо спосіб її обробки, агрегації та поширення істотно підвищує рівень втручання у

приватне життя, це свідчить про те, що в умовах цифровізації вирішальне значення має не лише зміст інформації, а й технологічний спосіб її використання.

Використання систем розпізнавання облич, технологій ШІ, прогнозування поведінки та автоматизованої ідентифікації осіб у публічному просторі особливо загострює питання дотримання не лише права на приватність, а й свободи мирних зібрань. У цифрову епоху втручання у права людини дедалі частіше здійснюється саме через алгоритмічні механізми обробки даних, що дозволяють державі здійснювати масштабний і прихований моніторинг поведінки осіб. Навіть за відсутності формальних обмежень, сама можливість такого спостереження здатна створювати раніше згаданий в пункті 2.1. «*стримувальний ефект*», який впливає на поведінку осіб і знижує їхню готовність реалізовувати свої права [68].

Показовою у цьому контексті є справа Glukhin v. russia [51], у якій заявника було ідентифіковано за допомогою технологій розпізнавання обличчя, що функціонують на основі алгоритмів ШІ. Для встановлення його особи правоохоронні органи використали поєднання цифрових джерел: зображення з відкритих онлайн-платформ, відеозаписи з камер спостереження, а також, імовірно, системи розпізнавання облич у режимі реального часу. Такі технології дозволяють не лише ідентифікувати особу, але й здійснювати автоматизоване зіставлення даних, відстеження переміщень та формування поведінкових моделей. Отримані таким чином дані були використані як докази у провадженні про адміністративне правопорушення.

ЄСПЛ встановив, що мало місце втручання у право заявника на повагу до приватного життя у розумінні статті 8 Конвенції [46]. Суд підкреслив, що застосування технологій ШІ у сфері спостереження якісно змінює характер втручання: воно стає більш інтенсивним, системним і потенційно всеохоплюючим. Біометричні дані, що обробляються за допомогою ШІ, дозволяють здійснювати ідентифікацію особи без її відома, аналізувати її поведінку та створювати детальні цифрові профілі, що значно підвищує ризики для приватності.

Ключовим у цій справі стало те, що втручання не відповідало вимозі «*якості закону*»: національне законодавство не містило достатньо чітких і передбачуваних правил щодо застосування таких технологій, не встановлювало меж їх використання та не передбачало ефективних гарантій проти зловживань, зокрема незалежного контролю чи судового дозволу. З урахуванням зазначеного, Суд дійшов висновку, що використання технологій

розпізнавання обличчя на основі штучного інтелекту у даному випадку не було «*необхідним у демократичному суспільстві*» [51].

Водночас ЄСПЛ звернув увагу на ширший контекст застосування таких технологій, підкресливши їхній потенційний вплив на інші фундаментальні права. Використання систем розпізнавання облич у ситуації, пов'язаній із реалізацією свободи вираження поглядів або участю у публічних заходах, здатне створювати стримувальний ефект щодо здійснення свободи зібрань – стаття 11 Конвенції, та свободи вираження поглядів – стаття 10 Конвенції [46]. Усвідомлення того, що будь-яка участь у публічній активності може бути зафіксована, проаналізована та використана проти особи, об'єктивно знижує рівень відкритості та громадянської активності.

У ширшому контексті зазначене рішення ЄСПЛ фактично стало судовим підтвердженням тих ризиків, які згодом отримали нормативне закріплення в праві Європейського Союзу. Зокрема, обмеження на використання систем масового біометричного розпізнавання, передбачені EU AI Act [65], відображають усвідомлення системної небезпеки таких технологій для приватності та інших фундаментальних прав людини.

З урахуванням проведеного аналізу практики ЄСПЛ, слід підкреслити, що в умовах зростання кіберзагроз захист цифрової приватності та персональних даних користувачів стає ключовим елементом демократичної безпеки. Через застосування ЄКПЛ Суд сформував ефективний інструментарій стримування надмірного цифрового втручання, утверджуючи персональні дані як фундаментальний елемент людської гідності та автономії.

Тобто практика ЄСПЛ не лише реагує на виклики цифрової реальності, але й активно формує правові межі допустимого використання технологій у сучасному швидкоплинному демократичному суспільстві. В умовах стрімкого розвитку інформаційно-телекомунікаційних технологій, які, з одного боку, розширюють можливості обробки даних, а з іншого — ускладнюють забезпечення цифрової приватності та індивідуальності особи в мережі Інтернет та інформаційному просторі, зростають ризики порушення права на приватність та втручання в приватне інформаційне життя особи.

2.3. Міжнародно-правові механізми контролю, забезпечення та відповідальності за порушення права на цифрову приватність у контексті протидії сучасним кіберзагрозам.

Питання ефективності захисту права на цифрову приватність сьогодні безпосередньо пов'язане з тим, як функціонують механізми його контролю, забезпечення та притягнення до відповідальності. На цьому рівні стає очевидним, що сама наявність міжнародно-правових стандартів не гарантує їх реального дотримання, особливо в умовах стрімкого розвитку цифрових технологій, інтенсифікації транснаціональних потоків даних та постійного зростання кіберзагроз. З огляду на раніше зазначене, цифровізація суспільних відносин виступає не лише технічним процесом, а чинником, який суттєво трансформує підходи до охорони права на приватність, що дедалі частіше реалізується саме у цифровому середовищі.

Проблема полягає в тому, що традиційна модель міжнародно-правового захисту, у межах якої ключовий акцент робився на судовому контролі та відповідальності держав, поступово втрачає свою ефективність. Цифрове середовище значно ускладнює як сам процес здійснення контролю, так і встановлення суб'єкта порушення. Обробка персональних даних відбувається одночасно в межах кількох юрисдикцій, а визначальну роль у цих процесах відіграють не лише держави, але й транснаціональні приватні компанії, які фактично контролюють значну частину глобальних інформаційних потоків.

У результаті механізми контролю та забезпечення права на приватність набувають розпорошеного і багаторівневого характеру. Вони реалізуються через поєднання різних інструментів — від діяльності міжнародних інституцій і національних регуляторів до внутрішніх політик самих компаній. Відсутність єдиного підходу до їх координації створює ситуацію, за якої ефективність захисту значною мірою залежить від конкретної юрисдикції або навіть від практики окремого органу, що, у свою чергу, зумовлює нерівномірність рівня гарантій цифрової приватності.

Стрімка цифровізація та зростання складності кіберзагроз додатково підсилюють дані виклики. Масове збирання персональних даних, транснаціональні програми спостереження, використання алгоритмічних систем і комерціалізація великих масивів даних функціонують за логікою, яка не узгоджується з класичною моделлю територіальної юрисдикції. Якщо раніше втручання у приватне життя здебільшого було локалізованим і прив'язаним до

конкретної держави, то сьогодні воно набуває розподіленого характеру, що ускладнює застосування традиційних правових механізмів.

Окремої уваги потребує питання контролю за діяльністю держав у сфері цифрового нагляду. Використання технологій масового збору даних, у тому числі під приводом забезпечення національної безпеки, нерідко виходить за межі ефективного міжнародного контролю. Існуючі механізми не завжди забезпечують належний рівень прозорості, а можливості притягнення держав до відповідальності залишаються обмеженими, що створює передумови для системних порушень права на приватність.

Не менш складною є ситуація з відповідальністю приватних суб'єктів. Транснаціональні технологічні компанії мають визначальний вплив на процеси обробки персональних даних, однак міжнародне право досі не сформувало універсальної моделі їхньої відповідальності. Як наслідок, це призводить до структурного дисбалансу: з одного боку, саме ці суб'єкти формують практику поводження з даними, а з іншого — механізми їх підзвітності залишаються фрагментарними та недостатньо узгодженими на міжнародному рівні.

За таких умов поступово формується інша логіка забезпечення права на цифрову приватність. Воно дедалі більше розглядається не лише як об'єкт нормативного захисту, а як елемент комплексної системи управління ризиками у глобальному кіберпросторі. Поряд із традиційними формами контролю зростає значення превентивних механізмів, регуляторного нагляду, а також технологічних інструментів, спрямованих на мінімізацію порушень ще до моменту їх виникнення. Враховуючи новизну та стрімку різноманітність кіберзагроз, дана систематика свідчить про перехід від реактивної моделі захисту до проактивної, в якій ключову роль відіграє не лише відповідальність за порушення, а й здатність правової системи запобігати таким порушенням у динамічному цифровому середовищі.

Однією з ключових інновацій сучасного європейського підходу до захисту персональних даних стала концепція екстериторіальної дії норм, найбільш повно втілена у Загальному регламенті про захист даних. Відповідно до статті 3 Регламенту [64], його положення застосовуються не лише до суб'єктів, заснованих на території Європейського

Союзу, але й до тих операторів і обробників даних, діяльність яких об'єктивно пов'язана з обробкою даних осіб, що перебувають у межах Союзу.

Насамперед, пункт 1 статті 3 прямо встановлює, що GDPR поширюється на «*опрацювання персональних даних у контексті діяльності осідку контролера або оператора в Союзі, незалежно від того, чи відбувається саме опрацювання в межах Союзу чи ні*» [64]. Таке формулювання є принципово відмінним від класичного територіального підходу, оскільки законодавець свідомо відмовляється від прив'язки до місця здійснення технічної обробки даних. Натомість визначальним стає функціональний зв'язок обробки із діяльністю відповідного осідку. У доктринальному вимірі це положення фактично закріплює пріоритет економічної та організаційної інтегрованості над формальною територіальністю, що дозволяє охоплювати ситуації, коли обробка даних здійснюється за межами ЄС, але в інтересах або в рамках діяльності суб'єкта, присутнього на його території.

Подальший розвиток цієї логіки міститься у пункті 2 статті 3, який встановлює, що Регламент застосовується до обробки персональних даних суб'єктів, «*які перебувають у Союзі*», навіть якщо контролер або оператор не має осідку в ЄС, за умови, що така обробка пов'язана:

a) з «*пропонуванням товарів чи наданням послуг*» таким особам, незалежно від факту оплати; або

b) з «*моніторингом їх поведінки, якщо така поведінка має місце в межах Союзу*» [64].

Саме зазначені два критерії — спрямованість діяльності (англ.: *offering of goods or services*) та відстеження поведінки (англ.: *monitoring of behaviour*) — формують матеріальний тест застосовності Регламенту. Варто підкреслити, що йдеться не про громадянство особи, а про її фактичне перебування на території ЄС, що суттєво розширює коло суб'єктів, на яких поширюється захист.

Як випливає з усталеної практики тлумачення цієї норми, сама по собі доступність вебресурсу на території ЄС не є достатньою підставою для застосування Регламенту. Вирішальним є наявність ознак цілеспрямованої діяльності — використання мови, валюти, логістики або інших елементів, які свідчать про орієнтацію на ринок Союзу. Аналогічно, критерій «*моніторингу поведінки*» охоплює, зокрема, використання технологій відстеження,

профілювання або аналізу онлайн-активності користувачів, що дозволяє робити висновки про їх уподобання чи поведінкові характеристики.

Окремо слід звернути увагу на пункт 3 статті 3, відповідно до якого GDPR застосовується до обробки персональних даних контролером, що не має осідку в Союзі, «*але в місці, де застосовується законодавство держави-члена в силу публічного міжнародного права*» [64]. Йдеться про класичні випадки екстериторіальної дії державної юрисдикції — дипломатичні представництва, консульські установи, судна або інші об'єкти, на які поширюється право відповідної держави. Хоча норма має більш вузьке практичне застосування, вона демонструє спадковість між традиційними інститутами міжнародного права та новими формами регулювання у цифровій сфері.

В сукупності наведені положення статті 3 [64] дозволяють констатувати, що її значення виходить далеко за межі технічного визначення сфери дії Регламенту. Фактично вона закріплює нову модель юрисдикції, яка ґрунтується не на території як такій, а на поєднанні функціонального, поведінкового та нормативного критеріїв.

Підхід знаменує відхід від класичного доктринального уявлення про територіальність права і формує нову модель нормативного контролю, засновану на прив'язці не до місця розташування суб'єкта, а до ринку, поведінки користувача та фактичного потоку даних. У науковій літературі така модель описується через категорії «*market-based jurisdiction*» та «*effects doctrine»*, відповідно до яких визначальним стає не формальний критерій юрисдикції, а реальний вплив діяльності на права осіб у межах певного правового простору.

Практична імплементація моделі найбільш яскраво проявляється у правозастосовній діяльності наглядових органів держав-членів ЄС в межах GDPR. Зокрема, показовими є рішення щодо притягнення до відповідальності транснаціональних технологічних корпорацій, які, не будучи формально обмеженими територією ЄС, здійснювали обробку персональних даних осіб, що перебувають у Союзі, або впливали на відповідні цифрові ринки.

Так, у 2019 році Національна комісія з інформатики та свобод Франції (CNIL) наклала штраф на компанію Google у розмірі 50 млн євро за порушення принципів прозорості та належної згоди користувачів. У подальшому практика застосування санкцій набула ще більшої інтенсивності та масштабності. У 2021 році Національна комісія із захисту даних

Люксембургу (CNPD) оштрафувала Amazon на 746 млн євро за порушення, пов'язані з обробкою персональних даних у контексті таргетованої реклами без належної правової підстави [71].

Найбільш резонансним став кейс 2023 року, коли Ірландська комісія із захисту даних (Data Protection Commission) наклала на Meta Platforms штраф у розмірі 1,2 млрд євро за незаконну передачу персональних даних користувачів з ЄС до Сполучених Штатів без забезпечення належного рівня їх захисту [60]. У рішенні було встановлено, що використання стандартних договірних положень (SCCs) не усувало ризиків для основоположних прав і свобод суб'єктів даних, зокрема у зв'язку з можливістю доступу до цих даних з боку іноземних органів державної влади.

Крім того, значні штрафи були накладені і в інших справах: зокрема, 405 млн євро щодо Meta за порушення правил обробки даних неповнолітніх, 390 млн євро — за відсутність належної правової підстави для персоналізованої реклами, а також 345 млн євро щодо TikTok за аналогічні порушення у сфері захисту даних дітей. Важливо відзначити, що значна частина перерахованих рішень ухвалювалася саме ірландським регулятором як головним наглядовим органом для багатьох технологічних компаній, зареєстрованих у цій юрисдикції.

Додатково, узагальнені статистичні дані, оприлюднені на офіційному аналітичному ресурсі Enforcement Tracker, який спеціалізується на систематизації практики правозастосування GDPR, свідчать про системний характер застосування фінансових санкцій у сфері захисту персональних даних.

Зосібна, серед найбільших штрафів домінують справи проти компаній Meta, TikTok, Amazon, LinkedIn та інших суб'єктів цифрової економіки, а підставами відповідальності найчастіше виступають відсутність належної правової підстави для обробки даних, недотримання принципів обробки, а також неналежне забезпечення технічних і організаційних заходів безпеки.

Для наочності зазначених тенденцій у **Додатку А** подано узагальнену таблицю найбільших штрафів, накладених за порушення вимог GDPR, що ілюструє як масштаби фінансової відповідальності, так і типові види правопорушень у даній сфері.

Важливо звернути увагу, що всі зазначені випадки об'єднує спільна риса: відповідні компанії є глобальними акторами цифрового ринку, діяльність яких не обмежується

територією ЄС, однак вони були піддані юрисдикції європейських регуляторів саме через наявність функціонального зв'язку з європейським ринком та користувачами. Наочно ілюструється, що екстериторіальність у межах GDPR не є лише формальною декларацією, а виступає реальним механізмом забезпечення дотримання прав людини у цифровому середовищі.

Окремо слід зазначити, що вказаний підхід отримав подальший розвиток на глобальному рівні: станом на сьогодні понад

120 держав світу імплементували або адаптували правові режими захисту персональних даних, орієнтовані на модель GDPR, зокрема Бразилія (General Personal Data Protection Law, LGPD) [50] та Індія (Digital Personal Data Protection Act, DPDP) [42]. Свідчить про трансформацію міжнародно-правової парадигми від класичного територіального принципу до функціонального підходу, у межах якого ключове значення має не місце здійснення обробки даних, а її фактичний вплив на права особи.

Більше того, наведена практика демонструє трансформацію самої природи контролю: санкції застосовуються не лише як реакція на вже вчинене порушення, але і як інструмент превентивного впливу на поведінку суб'єктів. Значні розміри штрафів виконують функцію стримування (англ.: *deterrence*), змушуючи компанії переглядати свої бізнес-моделі, впроваджувати політики захисту даних та інтегрувати відповідні гарантії у власні технологічні рішення.

Здебільшого, екстериторіальність постає не лише як технічний інструмент розширення юрисдикції, але як механізм примусу до глобального дотримання європейських стандартів цифрової приватності, що виконує функцію так званого «*нормативного експорту*» (англ.: *normative power Europe*) [64].

Характерною рисою сучасного режиму захисту цифрової приватності є запровадження концепції спільного забезпечення виконання (англ.: *composite enforcement)* — змішаного механізму контролю, у межах якого взаємодіють національні, наднаціональні та квазі-міжнародні інституції. У системі GDPR це виявляється у поєднанні повноважень національних органів із захисту даних, Європейської ради із захисту даних (англ.: European Data Protection Board, EDPB), а також Суду Європейського Союзу (англ.: Court of Justice of

the European Union, CJEU), який забезпечує уніфіковане тлумачення норм та формує обов'язкову для застосування практику.

Показовими у цьому контексті є справи Maximillian Schrems v Data Protection Commissioner [58] та Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [41], які стали ключовими орієнтирами для визначення правових меж транскордонної передачі персональних даних.

У справі Maximillian Schrems v Data Protection Commissioner (C-362/14, 2015) [58] Суд Європейського Союзу досліджував правомірність передачі персональних даних користувачів із Європейського Союзу до США в межах механізму Safe Harbor, запровадженого рішенням Європейської Комісії 2000/520. Фактичні обставини справи були пов'язані зі скаргою австрійського громадянина Максімілліана Шремса до ірландського наглядового органу, в якій він стверджував, що після викриттів щодо діяльності Агентства національної безпеки США (NSA) стало очевидним, що американське законодавство не забезпечує належного рівня захисту персональних даних від масового державного нагляду. Суд, аналізуючи положення Директиви 95/46/ЄС [43] та Хартії основоположних прав ЄС [30], дійшов висновку, що система Safe Harbor не гарантує «*еквівалентного рівня захисту*», оскільки дозволяє органам державної влади США здійснювати широкомасштабний доступ до персональних даних без належних обмежень, контролю та ефективних засобів правового захисту. У результаті рішення про адекватність було визнано недійсним, а також підтверджено, що національні наглядові органи зберігають повноваження перевіряти відповідність передачі даних вимогам права ЄС незалежно від рішень Комісії.

П'ять років потому розглядалася наступна суміжна справа Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (C-311/18, 2020) [41] де Суд ЄС розвинув цю правову позицію, розглядаючи законність використання стандартних договірних положень (англ.: Standard Contractual Clauses, SCCs) та механізму Privacy Shield для передачі даних до США. Суд визнав, що хоча SCCs як інструмент залишаються чинними, їх застосування не може бути формальним: контролери даних та наглядові органи зобов'язані оцінювати, чи забезпечує правова система третьої країни рівень захисту, «по суті еквівалентний» тому, що гарантується в ЄС. Водночас Суд визнав недійсним механізм Privacy Shield, оскільки він не усував системних ризиків доступу державних органів США до

персональних даних і не забезпечував ефективних засобів судового захисту для суб'єктів даних. Тобто, у даній справі було закріплено підхід, відповідно до якого ключовим критерієм правомірності міжнародної передачі даних є не лише формальна наявність правового інструменту, а й реальний рівень гарантій захисту прав людини.

Особливої уваги заслуговує механізм «*one-stop-shop*», передбачений статтею 56 GDPR [64], який покликаний забезпечити координацію діяльності національних наглядових органів у випадках транскордонної обробки даних. Його сутність полягає в тому, що провідну роль у розгляді справи відіграє наглядовий орган держави-члена, де розташований основний осідок контролера. З одного боку, це сприяє уніфікації практики та зменшенню адміністративного навантаження на бізнес, однак з іншого — виявило низку структурних проблем. Зокрема, значна кількість справ концентрується у юрисдикціях, де розміщені штаб-квартири великих технологічних компаній, передусім в Ірландії, що призводить до перевантаження відповідного наглядового органу, затягування процедур та неоднорідності правозастосування.

У контексті Ради Європи аналогічний композитний підхід спостерігається у межах Конвенції 108+ [31]. Ключову роль у її функціонуванні відіграє Консультативний комітет (T-PD), який здійснює тлумачення положень конвенції, виробляє рекомендації та сприяє гармонізації національних режимів. Хоча механізм Конвенції 108+ не передбачає прямих санкцій, його «*м'яка*» нормативна сила істотно впливає на формування стандартів у державах, що не входять до ЄС.

Попри формальну жорсткість санкційних механізмів (зокрема штрафи до 4% річного глобального обороту закріплені в статті 83 GDPR [64], практика свідчить про системну проблему «*under-enforcement*» – недостатнього та нерівномірного застосування норм про захист цифрової приватності. Причини даного явища мають комплексний характер і включають інституційну перевантаженість наглядових органів, асиметрію ресурсів між регуляторами та глобальними корпораціями, а також політичні міркування держав, зацікавлених у збереженні інвестиційної привабливості.

Практичним прикладом є численні скарги, подані правозахисними організаціями, зокрема Європейським центром цифрових прав (англ.: European Center for Digital Rights, NOYB) — незалежною неурядовою організацією, заснованою австрійським юристом

Максом Шремсом, діяльність якої спрямована на стратегічний судовий захист прав суб'єктів даних та забезпечення ефективного застосування норм GDPR. Організація активно ініціює провадження проти транснаціональних технологічних компаній, зокрема у сфері незаконних трансферів даних та поведінкового таргетингу. Водночас значна частина таких скарг роками перебуває на стадії розгляду без остаточного рішення, що додатково ілюструє проблему затягування процедур та обмеженої ефективності правозастосування.

Фундаментальним викликом для міжнародно-правових механізмів захисту цифрової приватності є детериторіалізація — розрив між формальними межами юрисдикції та фактичним функціонуванням цифрових інфраструктур. Використання хмарних технологій, розподілених серверів, глобальних платформ і систем штучного інтелекту унеможливлює однозначне визначення місця вчинення правопорушення та, відповідно, ускладнює застосування класичних колізійних прив'язок.

Показовим у цьому контексті є справи щодо компанії Clearview AI Inc. [47], яка здійснювала масове збирання зображень осіб шляхом Web scraping з відкритих інтернет-ресурсів та формувала біометричну базу даних для подальшого використання у системах розпізнавання облич. За результатами провадження, ініційованого національним органом Італії із захисту даних (італ.: Garante per la protezione dei dati personali), було встановлено порушення низки ключових положень GDPR, зокрема статей 5 – принципи обробки даних, 6 – правомірність обробки, 9 – обробка спеціальних категорій даних, 13–15 інформування суб'єктів даних та реалізація їхніх прав, а також статті 27 – обов'язок призначення представника в ЄС [64]. У 2022 році на компанію було накладено штраф у розмірі 20 млн євро, а також застосовано додаткові коригувальні заходи, включаючи заборону подальшої обробки даних та зобов'язання щодо їх видалення [47, 45].

Суттєвим є те, що навіть за відсутності фізичної присутності компанії на території Європейського Союзу, її діяльність була визнана такою, що підпадає під дію GDPR на підставі екстериторіального принципу – стаття 3 п. 2 GDPR [64], оскільки обробка даних була пов'язана з моніторингом поведінки осіб, які перебувають у ЄС. Підтверджується трансформація юрисдикційного підходу від територіального до функціонального.

У науковій літературі дана проблематика отримала ґрунтовне осмислення. Зокрема, у дослідженні Каміли Дул, аспірантки Школи права Університету королеви Мері Лондона,

«Facial Recognition Technology vs Privacy: The Case of Clearview AI» [45] обґрунтовується, що бізнес-модель Clearview AI, заснована на масовому спостереженні та агрегації біометричних даних, фактично вступає в конфлікт із сутністю фундаментального права на приватність. Авторка підкреслює, що традиційна «*вертикальна*» модель застосування прав людини (лише у відносинах держава — особа) є недостатньою в умовах цифрової економіки, де приватні корпорації набувають квазідержавних повноважень, що зумовлює необхідність розвитку «*горизонтального*» ефекту фундаментальних прав.

Спробою нормативної відповіді на виклики детериторіалізації є Регламент ЄС 2024/1689 від 13 червня 2024 року про встановлення гармонізованих правил щодо Штучного інтелекту (англ. скорочено: EU Artificial Intelligence Act, далі – EU AI Act, Регламент про ШІ) [65], яким вносяться зміни до низки регламентів і директив Європейського Союзу.

EU AI Act формує комплексну модель регулювання, що поєднує екстериторіальний підхід із превентивним контролем на етапі розробки та використання технологій.

Регламент про ШІ має широку сферу застосування та поширюється не лише на суб'єктів, що діють на території ЄС, але й на тих, хто розміщує або використовує системи штучного інтелекту поза межами Союзу, якщо результати їх функціонування використовуються в ЄС. Такий підхід фактично відтворює логіку GDPR щодо «*ефекту на ринку*» та «*поведінкового моніторингу*».

Ключовою особливістю Регламенту про ШІ є запровадження ризик-орієнтованої моделі, відповідно до якої всі системи штучного інтелекту поділяються на чотири категорії:

- системи з неприйнятним ризиком (заборонені);
- системи високого ризику (підлягають суворому регулюванню);
- системи обмеженого ризику (вимоги прозорості);
- системи мінімального ризику (мінімальне втручання).

Особливо жорсткі вимоги встановлюються для високоризикових систем, зокрема у сферах правосуддя, правоохоронної діяльності, працевлаштування, освіти та критичної інфраструктури. Системи підлягають обов'язковій оцінці впливу на фундаментальні права, впровадженню систем управління ризиками, забезпеченню якості даних, прозорості алгоритмів, а також людського контролю (англ.: *human oversight)* [65].

У сучасних умовах EU AI Act виступає як *lex specialis* щодо GDPR: він не замінює режим захисту персональних даних, а доповнює його шляхом регулювання технічних ризиків та класифікації систем штучного інтелекту [1]. Зокрема, станом на 2026 рік вже застосовуються норми щодо заборони окремих практик, таких як використання систем масового біометричного розпізнавання у публічних просторах за відсутності належних гарантій.

Окрему увагу приділено системам біометричної ідентифікації, які, як і у випадку справ щодо Clearview AI, визнаються високоризиковими. Використання дистанційної біометричної ідентифікації у публічних місцях для правоохоронних цілей загалом заборонено, за винятком вузько визначених випадків.

Регламент також встановлює значні санкції за порушення його вимог — до 35 млн євро або 7% річного глобального обороту компанії, що перевищує навіть максимальні штрафи, передбачені GDPR, які сягають всього 4% [23].

Водночас, незважаючи на прогресивність такого підходу, він не усуває базового структурного протиріччя між глобальною природою цифрових технологій та фрагментованістю міжнародно-правового регулювання. Навіть за умов екстериторіального застосування норм, їх ефективність залишається залежною від інституційної спроможності держав та рівня міжнародної координації.

Узагальнюючи викладене, доцільно зазначити, що сучасні міжнародно-правові механізми забезпечення цифрової приватності зазнають трансформації під впливом стрімкого розвитку цифрових технологій та змін у підходах до створення, обробки й використання даних. Незважаючи на поступове формування більш комплексних і адаптивних моделей правового регулювання, рівень їх практичної ефективності залишається неоднорідним та значною мірою залежить від інституційних можливостей держав, а також ефективності міжнародної співпраці. Особливо гостро зазначені проблеми проявляються в умовах зростання кіберзагроз і гібридних конфліктів, у межах яких порушення цифрової приватності набуває не лише правового, але й безпекового значення.

За таких обставин постає питання не стільки подальшого ускладнення нормативних конструкцій, скільки забезпечення їх дієвості у конкретному національному контексті. Відтак ключовим стає пошук ефективних моделей імплементації міжнародних стандартів,

здатних врахувати як глобальний характер цифрових процесів, так і специфіку внутрішніх викликів держави.

РОЗДІЛ 3
АДАПТАЦІЯ ЗАКОНОДАВСТВА УКРАЇНИ ДО МІЖНАРОДНО-ПРАВОВИХ СТАНДАРТІВ ЗАХИСТУ ЦИФРОВОЇ ПРИВАТНОСТІ ТА ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

3.1. Правове регулювання захисту персональних даних та реалізація права на цифрову приватність в Україні.

Формування інформаційного суспільства та інтенсивна цифровізація публічних і приватних сфер суспільного життя зумовили докорінну трансформацію правових підходів до розуміння приватного життя особи. Нинішні умови права на приватність дедалі більше пов’язується не лише з фізичною або комунікативною недоторканністю, а й із контролем особи над інформацією про себе, тобто над персональними даними. В Україні зазначена проблема набула особливої актуальності у зв’язку з упровадженням електронного урядування, функціонуванням численних державних реєстрів, розвитком цифрових сервісів та одночасним посиленням інформаційно-безпекових викликів в умовах воєнного стану. У таких обставинах захист персональних даних перестає бути вузькогалузевим інститутом і трансформується у комплексний міжгалузевий механізм забезпечення фундаментальних прав людини.

Водночас персональні дані виступають особливим інформаційним ресурсом, який може використовуватися для ідентифікації особи, встановлення її соціальних зв’язків, місця перебування, фінансового стану та інших характеристик, що обумовлює необхідність їх належного правового захисту від несанкціонованого доступу, використання, поширення чи знищення. В умовах розвитку цифрових технологій і зростання обсягів обробки інформації ризики порушення приватності значно підвищуються, що актуалізує потребу у формуванні ефективної системи правового регулювання у даній сфері.

Конституційно-правові засади захисту персональних даних в Україні мають визначальний характер та формують методологічну основу подальшого нормативного регулювання у відповідній сфері. На рівні Основного Закону закріплюються базові ціннісні орієнтири, що визначають зміст і спрямованість правового забезпечення права на

приватність, а також встановлюються межі допустимого втручання у сферу особистого життя.

Згідно зі статею 3 Конституції України (далі – КУ) [4] людина, її життя і здоров'я, честь, гідність, недоторканність і безпека визнаються найвищою соціальною цінністю, а права та свободи людини визначають основний зміст і спрямованість діяльності держави. З огляду на це, право на приватне життя слід розглядати як одну з базових конституційних гарантій забезпечення людської гідності та недоторканності особистої сфери людини. Виходячи з наведеного, право на приватне життя постає як один із ключових елементів людської гідності, що підлягає особливому конституційному захисту.

Подальшу конкретизацію зазначені положення знаходять у статті 32 КУ [4], яка закріплює гарантії невтручання в особисте і сімейне життя особи та встановлює заборону на збирання, зберігання, використання чи поширення конфіденційної інформації без передбачених законом підстав. У такий спосіб конституційне регулювання у сфері захисту персональних даних базується на принципі недоторканності приватної сфери людини та визнанні згоди особи однією з ключових передумов правомірної обробки її персональних даних.

Особливістю зазначеної норми є її комплексний характер, оскільки вона одночасно закріплює як суб'єктивне право особи на недоторканність приватного життя, так і визначає межі його обмеження. Допустимість втручання пов'язується виключно з наявністю закону та обґрунтуванням такого втручання легітимними цілями, зокрема інтересами національної безпеки, економічного добробуту та прав людини, що відповідає загальноєвропейським стандартам у сфері захисту персональних даних.

Положення статті 32 КУ [4] слід аналізувати не відокремлено, а у системному зв'язку зі статтею 34 КУ, яка закріплює гарантії свободи думки, слова та права особи на отримання, зберігання, використання і поширення інформації [4]. Співвідношення зазначених конституційних приписів формує необхідність узгодження інтересів щодо захисту приватної сфери людини з потребами держави та суспільства в інформаційній сфері. За таких умов ключового значення набуває дотримання принципу пропорційності, відповідно до якого втручання у приватне життя допускається лише за наявності належного правового обґрунтування, суспільної необхідності та відповідності легітимній меті.

Додаткового значення набуває проблема забезпечення такого балансу в умовах дії правового режиму воєнного стану. Відповідно до статті 64 КУ [4], конституційні права і свободи можуть бути обмежені лише у випадках, передбачених Конституцією, зокрема в умовах воєнного або надзвичайного стану, і лише в межах, визначених законом [4]. Вищезазначене вказує на неприпустимість довільного втручання у сферу персональних даних навіть у кризових умовах, підкреслюючи обов'язковість дотримання принципів законності, обґрунтованої необхідності та пропорційності.

Практика Конституційного Суду України відіграє визначальну роль у формуванні національних стандартів захисту персональних даних. У Рішенні від 30 жовтня 1997 року № 5-зп [15] Суд вперше заклав концептуальні засади розуміння конфіденційної інформації про особу, підкресливши, що забороняється не лише її збирання, а й *«…зберігання, використання та поширення… без її попередньої згоди*», за винятком випадків, прямо передбачених законом. Водночас до такої інформації віднесено, зокрема, відомості про стан здоров'я, сімейний стан, майнові характеристики та інші персональні дані, що окреслює широкий зміст цього поняття.

Подальшого розвитку зазначені підходи отримали у Рішенні від 20 січня 2012 року № 2-рп/2012 [14], у якому Суд здійснив системне тлумачення конституційних положень щодо права на приватність та інформацію. Зокрема, наголошено, що інформацією про особу є «*будь-які відомості… про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована*», а її обробка без згоди суб'єкта становить втручання в особисте і сімейне життя, допустиме лише у виключних, визначених законом випадках.

Сформульовані правові позиції дозволяють дійти висновку, що сам факт включення персональних даних до інформаційних систем чи державних реєстрів не змінює їх правової природи як конфіденційної інформації та не звільняє державу від обов'язку забезпечення належного рівня їх захисту. Зазначений підхід має фундаментальне значення для формування правового режиму обробки даних у цифровому середовищі та слугує орієнтиром для подальшого розвитку законодавства у сфері цифрової приватності.

Особливе значення у системі правового регулювання захисту персональних даних в Україні мають міжнародні договори, обов'язковість яких надана Верховною Радою України. Відповідно до статті 9 КУ [4], такі міжнародні договори є складовою частиною

національного законодавства, у зв'язку з чим їх положення підлягають застосуванню у внутрішньому правопорядку та враховуються під час тлумачення і реалізації норм національного права.

Важливе значення мають положення ЄКПЛ [46] та Конвенції Ради Європи № 108+ [31], які формують ключові орієнтири для визначення меж втручання у приватне життя та закріплюють основоположні принципи обробки персональних даних. Зокрема, йдеться про вимоги законності, пропорційності, цільового обмеження та належного рівня захисту інформації.

Імплементація зазначених міжнародних стандартів у національну правову систему забезпечує узгодженість правового регулювання із загальноєвропейськими підходами та підсилює гарантії захисту прав суб'єктів персональних даних. Їх застосування у національній правозастосовній практиці сприяє формуванню єдиного підходу до розуміння та реалізації права на цифрову приватність, що набуває особливої актуальності в умовах розвитку цифрових технологій та зростання кіберзагроз.

Подальша конкретизація конституційних положень здійснюється у спеціальному законодавстві, насамперед у ЗУ «Про захист персональних даних» [8]. Згідно зі статтею 2 Закону персональні дані визначаються як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована. У статті 6 Закону закріплено принципи обробки персональних даних, серед яких провідне значення мають принципи законності, цільового призначення та пропорційності. Закон встановлює, що обсяг і характер персональних даних мають бути адекватними визначеній меті їх обробки, що є прямим відображенням конституційних стандартів обмеження прав людини.

Центральне місце у системі інституційного контролю у сфері захисту персональних даних посідає Уповноважений Верховної Ради України з прав людини, який відповідно до ЗУ «Про Уповноваженого Верховної Ради України з прав людини» [12] здійснює парламентський контроль за додержанням конституційних прав і свобод людини і громадянина. Його діяльність у даній сфері конкретизується положеннями ЗУ «Про захист персональних даних», що наділяють Уповноваженого спеціальними повноваженнями, спрямованими на забезпечення ефективного нагляду та реагування на порушення законодавства про персональні дані.

Зокрема, відповідно до статті 23 ЗУ «Про захист персональних даних» [8] Уповноважений наділений широким колом контрольних, наглядових та нормотворчих повноважень. До них належить право розглядати звернення фізичних і юридичних осіб та приймати рішення за результатами їх розгляду; здійснювати планові та позапланові, виїзні й безвиїзні перевірки володільців і розпорядників персональних даних, у тому числі з доступом до приміщень, інформаційних систем, баз даних і документів, включаючи інформацію з обмеженим доступом. Важливим інструментом впливу є право видавати обов'язкові для виконання приписи щодо усунення порушень, зокрема вимагати зміни, видалення або знищення персональних даних, обмеження чи припинення їх обробки, а також заборони передачі третім особам.

Окрім контрольних функцій, Уповноважений здійснює нормативно-регуляторну та консультативну діяльність, зокрема затверджує підзаконні нормативно-правові акти у випадках, передбачених законом, надає роз'яснення та рекомендації щодо практичного застосування законодавства, а також бере участь у формуванні державної політики, звертаючись із пропозиціями до органів державної влади щодо вдосконалення правового регулювання у сфері захисту персональних даних. Важливим елементом його компетенції є також складання протоколів про адміністративні правопорушення та їх направлення до суду, що забезпечує реалізацію механізму юридичної відповідальності.

Суттєве значення має і міжнародний вимір діяльності Уповноваженого, який передбачає взаємодію з іноземними суб'єктами та участь у міжнародних організаціях у сфері захисту персональних даних, зокрема у контексті виконання міжнародних зобов'язань України. Результати здійснення контрольної діяльності системно відображаються у щорічній доповіді Уповноваженого про стан додержання прав і свобод людини, що включає окремий розділ щодо дотримання законодавства у сфері захисту персональних даних.

Поряд із інституційним контролем важливу роль відіграють положення статті 24 ЗУ «Про захист персональних даних» [8], які встановлюють обов'язки володільців, розпорядників персональних даних та третіх осіб щодо забезпечення належного рівня їх захисту. Закон прямо зобов'язує зазначених суб'єктів вживати організаційних і технічних заходів для запобігання випадковій втраті або знищенню даних, а також їх незаконній обробці чи доступу до них.

З метою інституціоналізації внутрішнього контролю у суб'єктів обробки персональних даних передбачено створення або визначення спеціальних структурних підрозділів чи відповідальних осіб, які організовують роботу із забезпечення захисту персональних даних. Такі підрозділи виконують консультативно-координаційні функції, інформують володільців і розпорядників про вимоги законодавства та взаємодіють з Уповноваженим у процесі запобігання та усунення порушень.

Окремо законодавець визначає, що фізичні особи — підприємці, а також представники окремих професій (зокрема лікарі, адвокати, нотаріуси) несуть персональну відповідальність за забезпечення захисту персональних даних, якими вони володіють, що підкреслює універсальний характер обов'язку дотримання вимог інформаційної безпеки.

Законодавче регулювання інформаційних відносин в Україні характеризується комплексністю та взаємодоповнюваністю нормативно-правових актів, ключове місце серед яких також посідає ЗУ «Про інформацію» [9]. Згаданий Закон формує базові засади правового режиму інформації, у тому числі визначає гарантії захисту персональних даних та межі їх правомірного використання.

Зокрема, положення статті 11 закріплюють фундаментальне право фізичної особи на інформацію про себе, визначаючи персональні дані як відомості або сукупність відомостей, за допомогою яких особа є ідентифікованою або може бути ідентифікована. Важливою гарантією виступає встановлена заборона на збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, за винятком випадків, прямо передбачених законом і обумовлених необхідністю захисту національної безпеки, економічного добробуту та прав людини. Такий підхід відображає загальноєвропейські стандарти у сфері захисту приватності, зокрема принципи законності, цільового обмеження та пропорційності обробки даних.

На додаток законодавець деталізує зміст конфіденційної інформації, відносячи до неї, зокрема, відомості про національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також персональні ідентифікаційні дані (адресу, дату і місце народження). Водночас гарантується право кожного на вільний доступ до інформації, що стосується його особисто, що є важливою складовою реалізації права на приватність і інформаційне самовизначення.

Окрему увагу слід звернути на передбачені законом винятки із загального правила необхідності згоди суб'єкта персональних даних. Зокрема, у сфері здійснення верифікації та моніторингу державних виплат уповноважений центральний орган виконавчої влади має право обробляти персональні дані без отримання такої згоди, що свідчить про прагнення законодавця забезпечити баланс між інтересами держави та правами особи.

У системному зв'язку із ЗУ «Про доступ до публічної інформації» [7] формується цілісний механізм балансування між принципом відкритості діяльності суб'єктів владних повноважень та необхідністю захисту персональних даних. Ключове значення у цьому контексті має частина друга статті 6 зазначеного Закону [7], яка закріплює так званий «трискладовий тест» обмеження доступу до інформації. Відповідно до нього обмеження доступу є правомірним лише за умови одночасного дотримання трьох критеріїв:

1. наявності легітимної мети (зокрема, захист національної безпеки, громадського порядку, прав та репутації інших осіб);
2. існування реальної загрози заподіяння істотної шкоди таким інтересам у разі розголошення інформації;
3. переважання потенційної шкоди над суспільним інтересом в отриманні відповідної інформації.

Разом з тим ЗУ «Про доступ до публічної інформації» [7] містить низку важливих гарантій відкритості, зокрема встановлює перелік відомостей, доступ до яких не може бути обмежено. До них, серед іншого, належить інформація про використання бюджетних коштів, розпорядження державним і комунальним майном, результати перевірок та службових розслідувань, а також відомості, що містяться у деклараціях осіб, уповноважених на виконання функцій держави. Дана систематика спрямована на забезпечення прозорості публічної влади та запобігання корупційним ризикам.

Крім того, принципово важливим є положення про те, що обмеженню підлягає не документ як такий, а лише інформація, яка в ньому міститься. Твердження означає, що розпорядник інформації зобов'язаний надавати доступ до відкритої частини документа, вилучаючи або ретушуючи відомості з обмеженим доступом, що відповідає міжнародним стандартам у сфері доступу до інформації.

Окремим елементом правового механізму виступають положення щодо юридичної відповідальності за порушення законодавства про інформацію, закріплені у статті 27 ЗУ «Про інформацію» [9]. Вони передбачають можливість притягнення винних осіб до дисциплінарної, цивільно-правової, адміністративної або кримінальної відповідальності, що забезпечує належний рівень правового захисту та виступає превентивним засобом недопущення зловживань у сфері обробки інформації.

Істотну роль у забезпеченні права на захист персональних даних відіграють норми цивільного законодавства, які формують приватноправовий вимір охорони цифрової приватності та забезпечують ефективні механізми судового захисту. Передусім, Цивільний кодекс України (далі – ЦКУ) [19] закріплює систему особистих немайнових прав, у межах якої персональні дані розглядаються як складова права на повагу до приватного життя.

Згідно зі статтею 270 ЦКУ [19], фізичній особі гарантується система особистих немайнових прав, важливе місце серед яких у контексті захисту персональних даних посідають право на недоторканність приватного і сімейного життя, право на повагу до честі та гідності, а також право на таємницю листування й інших видів комунікації. З огляду на це, законодавець прямо підкреслює, що перелік таких прав не є вичерпним, що свідчить про відкритий характер цієї категорії та можливість її розвитку відповідно до сучасних викликів, зокрема у сфері цифровізації та обробки персональних даних.

Зміст права на приватність деталізується у статті 301 ЦКУ [19], відповідно до якої фізична особа самостійно визначає межі свого особистого життя та порядок доступу інших осіб до інформації про нього. Норма також гарантує право на збереження конфіденційності відомостей, що стосуються приватної сфери особи, а їх поширення допускається лише за згодою особи або у випадках, прямо встановлених законом.

Стаття 302 ЦКУ [19], у свою чергу, встановлює загальні засади реалізації права на інформацію, поєднуючи свободу інформаційної діяльності з необхідністю дотримання приватності. Зокрема, передбачено, що «збира*ння, зберігання, використання і поширення інформації про особисте життя фізичної особи без її згоди не допускаються*» [19], за винятком випадків, визначених законом і обумовлених легітимною метою, такою як захист національної безпеки, економічного добробуту та прав людини. Водночас особа, яка поширює інформацію, зобов’язана перевіряти її достовірність, що є проявом принципу

добросовісності у цивільних правовідносинах, за винятком інформації, отриманої з офіційних джерел, щодо якої встановлено спеціальний правовий режим [19].

У цивільно-правовому аспекті персональні дані розглядаються як немайнове благо, порушення якого тягне за собою виникнення права на захист, у тому числі шляхом звернення до суду. Такий захист може включати вимоги про припинення порушення, спростування недостовірної інформації, видалення чи обмеження доступу до персональних даних, а також відшкодування моральної шкоди незалежно від наявності матеріальних збитків.

Кримінально-правовий захист права на приватність і персональні дані в Україні забезпечується, зокрема, положеннями статті 182 Кримінального кодексу України (далі – ККУ) [5], яка встановлює відповідальність за порушення недоторканності приватного життя. У межах цієї норми законодавець криміналізує незаконне збирання, зберігання, використання, знищення, поширення або зміну конфіденційної інформації про особу, визнаючи такі дії суспільно небезпечними та такими, що посягають на фундаментальні права і свободи людини.

Об’єктивна сторона цього кримінального правопорушення охоплює широкий спектр протиправних діянь, пов’язаних із неправомірним обігом персональних даних, що свідчить про комплексний підхід законодавця до захисту інформаційної приватності. При цьому ключовим критерієм протиправності є відсутність законних підстав для обробки відповідної інформації, зокрема згоди особи або іншої передбаченої законом підстави. Водночас чинні санкції, передбачені статтею 182 ККУ [5] та статтею 188-39 КУпАП [3], залишаються недостатньо ефективними порівняно з підходами, закріпленими у GDPR [64], де розмір штрафів може сягати 20 млн євро або 4 % глобального річного обороту компанії.

Санкції за вчинення таких діянь мають альтернативний характер і передбачають можливість застосування як майнових, так і немайнових заходів впливу — від штрафу до обмеження волі, що забезпечує індивідуалізацію кримінальної відповідальності залежно від обставин справи. Кваліфікуючими ознаками складу правопорушення є повторність вчинення діяння або заподіяння істотної шкоди правам, свободам та інтересам особи, що зумовлює посилення кримінально-правових санкцій, включаючи можливість позбавлення волі [5].

Водночас законодавець визначає межі криміналізації, встановлюючи, що суспільно корисна діяльність, пов'язана з повідомленням про правопорушення (зокрема через засоби масової інформації або інші публічні канали) за умови дотримання вимог закону, не утворює складу цього кримінального правопорушення.

Адміністративно-правовий механізм забезпечення захисту персональних даних в Україні є важливою складовою загальної системи гарантій інформаційної безпеки та реалізується, зокрема, через норми Кодексу України про адміністративні правопорушення (далі – КУпАП), які встановлюють відповідальність за порушення законодавства у відповідній сфері.

Важливе місце у механізмі адміністративно-правового захисту персональних даних займає стаття 188-39 Кодексу України про адміністративні правопорушення [3], яка встановлює відповідальність за порушення вимог законодавства у відповідній сфері. Нормою передбачено диференційований підхід до визначення санкцій залежно від характеру вчиненого правопорушення та ступеня його суспільної шкідливості.

До адміністративних правопорушень у даній парадигмі, віднесено неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про здійснення обробки персональних даних, неподання змін до відповідних відомостей, а також надання неповної чи недостовірної інформації. За вчинення зазначених дій законодавством передбачено адміністративні штрафи як для громадян, так і для посадових осіб та фізичних осіб — підприємців.

Окремим складом адміністративного правопорушення визначено невиконання законних вимог або приписів Уповноваженого Верховної Ради України з прав людини щодо усунення порушень законодавства про захист персональних даних. За такі дії встановлено більш суворі санкції, що обумовлено підвищеним ступенем суспільної небезпеки відповідного правопорушення.

КУпАП [3] також передбачає підвищення відповідальності у випадку повторного вчинення аналогічних порушень протягом року після застосування адміністративного стягнення. Крім того, самостійним складом правопорушення визнається недотримання встановленого порядку захисту персональних даних, якщо це призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних.

Окремо законодавством передбачено адміністративну відповідальність за порушення встановлених вимог щодо забезпечення захисту персональних даних, якщо такі дії спричинили незаконний доступ до відповідної інформації або порушення прав суб'єкта персональних даних. За вчинення таких правопорушень КУпАП [3] встановлює застосування штрафних санкцій до громадян, посадових осіб та суб'єктів підприємницької діяльності, причому у разі повторного вчинення порушення протягом року розмір адміністративної відповідальності істотно посилюється.

Значний вплив на правове регулювання захисту персональних даних справляє також законодавство у сфері кібербезпеки, яке формує технологічне та організаційне підґрунтя забезпечення інформаційної безпеки. Зокрема, ЗУ «Про основні засади забезпечення кібербезпеки України» [10] визначає інформаційні ресурси, що містять персональні дані, як об'єкти кіберзахисту та покладає на державу, а також на суб'єктів забезпечення кібербезпеки, обов'язок впроваджувати комплекс заходів, спрямованих на запобігання несанкціонованому доступу, витоку, втраті чи модифікації інформації.

Оперуючись твердженнями, захист персональних даних виходить за межі суто правового регулювання та набуває міждисциплінарного характеру, поєднуючи правові, організаційні та технічні інструменти. Закон акцентує увагу на необхідності функціонування ефективної національної системи кібербезпеки, що охоплює як державні органи, так і суб'єктів приватного сектору, які обробляють значні масиви персональних даних.

Особливої актуальності зазначене регулювання набуває в умовах воєнного стану, коли зростає кількість і складність кіберзагроз, спрямованих на критичну інформаційну інфраструктуру, державні реєстри та бази персональних даних. За таких умовах персональні дані стають не лише об'єктом приватноправового захисту, але й елементом національної безпеки, а їх компрометація може мати масштабні наслідки як для окремих осіб, так і для держави в цілому.

Отже, правове регулювання захисту персональних даних та реалізації права на цифрову приватність в Україні постає як складна, багаторівнева та динамічна система, що формується на перетині конституційних приписів, норм галузевого законодавства, підзаконного регулювання та практики їх застосування. Її специфіка полягає у поєднанні публічно-правових і приватноправових механізмів, які у своїй сукупності забезпечують як

превентивний контроль за обробкою персональних даних, так і ефективний захист порушених прав особи.

Водночас ефективність системи визначається не лише нормативною розвиненістю, але й здатністю держави забезпечити її належну реалізацію в умовах постійних трансформацій цифрового середовища. Ключовим залишається досягнення збалансованого співвідношення між правом на приватність і публічними інтересами, зокрема у сфері національної безпеки, що потребує гнучкого та водночас правомірного підходу до обмеження прав людини.

Особливої актуальності ці питання набувають в умовах воєнного стану, коли різко зростає інтенсивність обробки персональних даних, розширюється коло суб'єктів, які мають до них доступ, а також підвищується рівень кіберзагроз і ризиків несанкціонованого втручання. Війна зумовлює необхідність оперативного обміну інформацією, створення нових реєстрів, використання цифрових технологій у сфері безпеки та оборони, що, у свою чергу, породжує низку правових викликів, пов'язаних із забезпеченням конфіденційності, недопущенням зловживань та гарантуванням прав суб'єктів персональних даних.

3.2. Особливості забезпечення конфіденційності персональних даних в Україні в умовах воєнного стану з урахуванням міжнародних стандартів кібербезпеки.

Запровадження правового режиму воєнного стану в Україні у зв'язку з повномасштабною збройною агресією рф було здійснено на підставі Указу Президента України від 24 лютого 2022 року № 64/2022 [6], виданого відповідно до статті 64 КУ [4]. Введення зазначеного спеціального правового режиму обумовило можливість тимчасового обмеження окремих конституційних прав і свобод людини та громадянина в межах, необхідних для забезпечення національної безпеки, територіальної цілісності та оборони держави. До таких прав належать і гарантії, передбачені статтею 32 КУ [4], що охоплюють сферу приватного і сімейного життя, а також питання захисту персональних даних.

Нормативний зміст статті 32 КУ [4] закріплює принцип недопустимості свавільного втручання у приватну сферу особи та встановлює заборону на збирання, зберігання, використання і поширення конфіденційної інформації про особу без її згоди, за винятком випадків, прямо визначених законом. При цьому навіть в умовах дії воєнного стану реалізація заходів, пов'язаних з обмеженням права на приватність або обробкою

персональних даних, повинна здійснюватися виключно на законних підставах і відповідати принципам необхідності, пропорційності та легітимної мети.

Воєнний стан істотно трансформував підходи до забезпечення конституційних прав і свобод людини в Україні, актуалізувавши проблему співвідношення між інтересами національної безпеки та гарантіями цифрової приватності. В умовах війни інформація про особу набуває подвійного значення: з одного боку, вона залишається об'єктом основоположного права людини, з іншого — перетворюється на критично важливий ресурс безпеки, який може бути використаний як для захисту держави, так і як інструмент ворожого впливу. Дана дихотомія зумовлює необхідність постійного балансування між потребами національної безпеки та обов'язком держави гарантувати мінімально необхідний рівень захисту приватності.

Відповідні підходи знаходять своє відображення і в міжнародно-правових актах у сфері захисту прав людини та персональних даних. Зокрема, стаття 8 ЄКПЛ [46] встановлює, що втручання у сферу приватного і сімейного життя допускається лише за умови його законності, наявності легітимної мети та необхідності у демократичному суспільстві. Серед підстав для такого втручання Конвенція визначає, зокрема, інтереси національної та громадської безпеки, економічного добробуту держави, а також потребу у захисті прав і свобод інших осіб. Поряд із цим стаття 15 Конвенції [46] передбачає право держави на тимчасовий відступ від окремих зобов'язань у період війни чи надзвичайної суспільної небезпеки, однак виключно в межах, обумовлених характером і масштабом відповідних обставин [46].

Міжнародні стандарти у сфері захисту персональних даних також допускають можливість встановлення певних обмежень у виняткових умовах. Так, Конвенція 108+ [31] передбачає можливість відступу від окремих принципів обробки персональних даних у випадках, коли це необхідно для забезпечення державної безпеки, громадського порядку, фінансових інтересів держави або захисту прав і свобод інших осіб.

На внутрішньодержавному рівні важливе місце у формуванні механізмів захисту персональних даних в умовах воєнного стану займає Закон України «Про основні засади забезпечення кібербезпеки України» [10]. У статті 1 зазначеного Закону кібербезпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави

у кіберпросторі, що охоплює також забезпечення належного рівня охорони персональних даних та конфіденційної інформації.

Згідно зі статтею 2 Закону [10], об'єктами кібербезпеки є, зокрема, права і свободи людини і громадянина, що підкреслює включення права на приватність і захист персональних даних до системи національної безпеки. У свою чергу, стаття 3 визначає основні принципи забезпечення кібербезпеки, серед яких — верховенство права, дотримання прав і свобод людини, пропорційність та адекватність заходів захисту, що кореспондує з конституційними вимогами та міжнародними стандартами [10].

Особливе значення має стаття 4 Закону, яка закріплює пріоритетність захисту прав і свобод людини при здійсненні заходів у сфері кібербезпеки. Означає, що навіть в умовах воєнного стану діяльність суб'єктів забезпечення кібербезпеки повинна здійснюватися з урахуванням необхідності мінімізації втручання у приватне життя особи [10].

Водночас стаття 5 визначає систему суб'єктів забезпечення кібербезпеки, до якої належать, зокрема, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України та інші органи. В межах своїх повноважень вони здійснюють заходи щодо запобігання, виявлення та реагування на кіберінциденти, що може передбачати обробку персональних даних без згоди особи — однак виключно на підставі закону та в межах національної безпеки.

Крім того, відповідно до статті 6 Закону, одним із основних напрямів державної політики у сфері кібербезпеки є забезпечення кіберзахисту інформаційних ресурсів, у тому числі державних інформаційних систем і реєстрів, які містять персональні дані. В умовах воєнного стану такі системи стають об'єктами підвищеного ризику кібератак, що обумовлює необхідність посилених заходів захисту.

Підтвердження міститься в аналітичних матеріалах Європейського парламенту, підготовленими в межах дослідницької служби EPRS, у яких наголошується, що кіберпростір у контексті агресії рф проти України трансформувався у повноцінне поле ведення війни. Зокрема, у дослідженні «The role of cyber in the russian war against Ukraine» [44] підкреслюється, що кібероперації використовуються поряд із традиційними військовими засобами та спрямовані як на підрив функціонування державних інституцій, так і на вплив на цивільне населення.

Додатково, у брифінгу «russia's war on Ukraine: Timeline of cyber-attacks» [67] акцентується, що кібератаки мали системний характер ще до початку повномасштабного вторгнення та супроводжують усі етапи збройної агресії. У документі детально простежується ескалація кібератак, спрямованих на державні органи, фінансові установи та об'єкти критичної інфраструктури України, що свідчить про їх інтегрованість у загальну стратегію гібридної війни.

Водночас війна як соціально-правовий феномен істотно підвищує ризики порушення конфіденційності персональних даних, що зумовлено трансформацією кіберпростору на повноцінний театр воєнних дій. У сучасних збройних конфліктах інформаційний та кібернетичний виміри фактично прирівнюються до традиційних форм ведення бойових дій, а персональні дані набувають стратегічного значення як об'єкт атак і водночас інструмент впливу.

Гібридний характер агресії рф зумовив системне застосування широкого спектра кібероперацій, спрямованих насамперед на українські державні інституції, об'єкти критичної інфраструктури та суб'єктів, що обробляють значні масиви персональних даних, а також безпосередньо на цивільне населення. За даними міжнародного аналітичного дослідження Cyber Dimensions of the Armed Conflict in Ukraine [38], у період з січня 2022 року по вересень 2023 року було зафіксовано щонайменше 574 кібератаки і кібероперації, спрямовані проти українських суб'єктів у 23 секторах економіки та публічного управління. Така інтенсивність кібератак свідчить про їх системний і цілеспрямований характер, а також про підвищений рівень загроз для обробки, збереження та захисту персональних даних в Україні.

Аналіз зазначених атак дозволяє виокремити кілька ключових напрямів впливу на інформаційну безпеку та приватність.

По-перше, значного поширення набули атаки, спрямовані на знищення даних або виведення з ладу інформаційних систем. Використання так званого «*wiper*»-шкідливого програмного забезпечення призводило до безповоротного видалення інформації з державних реєстрів та інформаційних систем, що створювало ризики втрати персональних даних і унеможливлювало їх відновлення без наявності резервних копій.

По-друге, суттєвий вплив мали кібератаки, спрямовані на порушення функціонування інформаційних сервісів, зокрема масові DDoS-атаки (англ.: Distributed Denial of Service —

розподілені атаки відмови в обслуговуванні) на державні портали та цифрові платформи. Такі дії призводили до тимчасової недоступності публічних послуг, що особливо критично в умовах воєнного стану, коли цифрові сервіси забезпечують доступ громадян до адміністративних, фінансових і соціальних послуг, пов'язаних з обробкою персональних даних.

По-третє, окрему загрозу становить використання персональних даних як об'єкта кіберрозвідки та інструменту впливу. У межах таких операцій здійснюється несанкціоноване отримання доступу до баз даних, їх копіювання, викрадення та подальше використання з розвідувальною або дестабілізаційною метою. При цьому персональні дані можуть застосовуватися для ідентифікації осіб, здійснення тиску, маніпуляцій або створення загроз їхній безпеці.

Крім того, значного поширення набули інформаційно-психологічні операції, пов'язані з дезінформацією та пропагандою. Вони реалізуються через різні канали — від масових SMS-кампаній до зламу медіаресурсів і поширення фальсифікованого контенту, зокрема із застосуванням технологій дипфейку. У таких випадках персональні дані можуть використовуватися для таргетування аудиторій, підвищення довіри до неправдивої інформації та посилення психологічного впливу.

Водночас Україна реалізувала передбачений міжнародним правом механізм відступу від окремих зобов'язань у сфері прав людини. Уряд України у 2022 році офіційно повідомив Генерального секретаря РЄ про відступ від окремих положень Європейської конвенції з прав людини відповідно до статті 15 Конвенції [46, 66]. У подальшому, у 2024 році, Україна подала оновлене повідомлення про обсяг та характер таких відступів, чітко вказавши, що вони мають тимчасовий характер, зумовлені виключно воєнною необхідністю та не зачіпають сутнісне ядро права на людську гідність [66].

Однією з найсерйозніших загроз для конфіденційності персональних даних в умовах війни є їх незаконний збір та використання на тимчасово окупованих територіях. За даними правозахисних та державних аналітичних джерел, окупаційні адміністрації здійснюють систематичний збір персональних даних громадян України шляхом примусової паспортизації, проведення так званих «*фільтраційних*» процедур, а також встановлення контролю над телекомунікаційною інфраструктурою, що зумовлює реальні ризики

подальшого використання таких даних для репресій, депортацій, переслідування та інформаційного тиску.

Суттєву небезпеку для персональних даних становлять також кіберзлочини та інформаційно-психологічні операції, що активно використовують відкриті джерела інформації, зокрема соціальні мережі. Аналітичні звіти Державної служби спеціального зв'язку та захисту інформації України та CERT-UA, зокрема доповідь «russia's Cyber Tactics H1'2023» [70], свідчать про суттєве зростання інтенсивності кіберінцидентів: у першій половині 2023 року їх кількість зросла більш ніж удвічі (в середньому до 4–5 інцидентів щоденно). Значна частина атак мала розвідувальний характер і була спрямована на отримання доступу до чутливих даних державних органів, правоохоронних структур та медіа.

У звіті підкреслюється, що російські кіберугруповання активно застосовують тактику швидкого вилучення даних (англ.: *data exfiltration*) — інколи протягом перших 30 хвилин після компрометації системи здійснюється копіювання тисяч документів та облікових даних користувачів. Водночас значна увага приділяється використанню фішингових кампаній і збору інформації з відкритих профілів, що дозволяє здійснювати таргетовані атаки, маніпулювати поведінкою користувачів та посилювати ефективність інформаційного впливу.

Крім того, зафіксовано систематичне використання викрадених персональних даних у так званих «*hack-and-leak*» операціях, спрямованих на дискредитацію державних інституцій, медіа та окремих осіб. Така практика свідчить про інтеграцію кіберінструментів у ширшу стратегію гібридної війни, де персональні дані виступають не лише об'єктом злочинного посягання, але й інструментом впливу.

Оперуючись аналізом слід підсумувати, що в умовах воєнного стану забезпечення конфіденційності персональних даних в Україні характеризується підвищеною складністю, що обумовлена необхідністю поєднання безпекових інтересів держави із гарантіями основоположних прав людини. Запровадження тимчасових обмежень права на приватність є допустимим лише за наявності чітких правових підстав і за умови дотримання принципів необхідності, пропорційності та правової визначеності, що відповідає як конституційним вимогам, так і міжнародно-правовим стандартам.

Національна модель правового регулювання, зокрема у сфері кібербезпеки, демонструє інтеграцію захисту персональних даних у ширший контекст національної безпеки, що є об'єктивною відповіддю на сучасні кіберзагрози та гібридний характер збройної агресії. Водночас практика свідчить про зростання ризиків порушення конфіденційності персональних даних, пов'язаних із кібератаками, незаконним збором даних, інформаційно-психологічними операціями та використанням персональної інформації як інструменту впливу.

За таких умов особливої актуальності набуває питання подальшого вдосконалення правового регулювання у даній сфері. Попри наявність базових нормативних механізмів, сучасні виклики засвідчують необхідність їх адаптації до нових реалій цифрової безпеки та узгодження із передовими міжнародними стандартами. З огляду на євроінтеграційний курс України, ключовим напрямом розвитку національної правової системи стає гармонізація законодавства у сфері захисту персональних даних із правом Європейського Союзу, що передбачає імплементацію високих стандартів цифрової приватності, ефективних механізмів контролю за обробкою даних та посилення інституційної спроможності у сфері їх захисту.

3.3. Перспективи гармонізації законодавства України з правом Європейського Союзу у сфері захисту персональних даних та цифрової приватності.

Європейська інтеграція України в сучасних умовах набуває не лише політико-правового, але й глибокого цивілізаційного значення, виступаючи системним чинником трансформації національної правової системи відповідно до європейських цінностей. Актуальність гармонізації законодавства у сфері захисту персональних даних істотно посилюється під впливом геополітичних змін, зумовлених повномасштабною війною, інтенсивною цифровізацією державного управління, а також трансформацією суспільного запиту на безпеку, довіру до державних інституцій та належний рівень захисту приватності.

Євроінтеграційні процеси зумовлюють трансформацію підходів до захисту персональних даних, унаслідок чого це питання виходить за межі технічного правового регулювання та інтегрується у систему базових засад демократичного розвитку держави.

Право ЄС щодо захисту персональних даних визнається фундаментальним правом, закріпленим, зокрема, у статті 8 Хартії основоположних прав ЄС [30] та статті 16 Договору про функціонування ЄС [72]. Відповідно, для держав-кандидатів досягнення належного

рівня захисту персональних даних розглядається як одна з ключових передумов подальшого просування на шляху до членства в ЄС.

Нормативною основою правової інтеграції України до Європейського Союзу є зобов'язання, що випливають з Угоди про асоціацію між Україною та Європейським Союзом [17], підписаної 27 червня 2014 року та ратифікованої Законом України від 16 вересня 2014 року № 1678-VII [11]. Зазначений міжнародно-правовий акт визначає стратегічний напрям поступового наближення національного законодавства України до *acquis communautaire* — сукупності правових норм, принципів і зобов'язань ЄС обов'язкових для держав-членів. Гармонізація законодавства у сфері захисту персональних даних не обмежується формальним запозиченням європейських норм, а передбачає комплексну трансформацію правової системи, що охоплює створення ефективних інституційних механізмів, забезпечення належного правозастосування та досягнення їх практичної дієвості.

Якісно новий етап євроінтеграційного процесу розпочався після подання Україною 28 лютого 2022 року заявки на вступ до Європейського Союзу та надання їй 23 червня 2022 року статусу держави-кандидата [73]. Подальшим кроком стало ухвалення у грудні 2023 року рішення про відкриття переговорів щодо вступу, а також проведення 25 червня 2024 року першої міжурядової конференції, що формально започаткувала переговорний процес. У межах переговорної рамки питання захисту персональних даних віднесено до кластеру «Основи», який відкривається на початковому етапі переговорів і закривається на завершальному, що свідчить про його фундаментальне значення для всієї системи євроінтеграційних перетворень України [73].

Порівняльний аналіз чинного ЗУ «Про захист персональних даних» [8] та GDPR [64] дає підстави констатувати не лише формальну наближеність окремих правових конструкцій, але й наявність глибинних концептуальних, інституційних і функціональних відмінностей, що зумовлюють різний рівень ефективності правового регулювання у відповідних правопорядках.

Насамперед, відмінності проявляються на рівні принципів обробки персональних даних. Хоча українське законодавство закріплює базові засади, зокрема законність, цільове призначення обробки та пропорційність, GDPR забезпечує їх значно вищий рівень

деталізації та практичної застосовності. Особливого значення набуває принцип підзвітності (англ.: *accountability*), відповідно до якого контролер не лише зобов'язаний дотримуватися вимог законодавства, але й має бути здатним довести таке дотримання через впровадження внутрішніх політик, процедур та механізмів контролю. У національному праві відповідний підхід має фрагментарний характер і не формує цілісної системи відповідальності, що негативно впливає на рівень комплаєнсу у сфері захисту персональних даних.

Другим ключовим аспектом є обсяг і ефективність гарантій прав суб'єкта персональних даних. GDPR встановлює розширений та деталізований каталог прав, включаючи «*право бути забутим*», право на обмеження обробки, право на перенесення даних, а також право на заперечення проти обробки [64]. Водночас особливістю є не лише нормативне закріплення цих прав, але й наявність чітких процедур їх реалізації, включаючи строки реагування, обов'язки контролера щодо інформування та механізми оскарження. На відміну від цього, ЗУ «Про захист персональних даних» [8] містить лише базовий перелік прав, який не супроводжується належною процедурною деталізацією, що суттєво обмежує можливість їх ефективної реалізації на практиці.

Суттєві розбіжності простежуються також у регулюванні автоматизованого прийняття рішень і профілювання, що набуває особливої актуальності в умовах стрімкого розвитку систем штучного інтелекту. GDPR, зокрема стаття 22 [64] встановлює право особи не підпадати під рішення, що ґрунтується виключно на автоматизованій обробці, якщо таке рішення має юридичні або інші істотні наслідки, а також передбачає обов'язок контролера забезпечити прозорість таких процесів шляхом надання інформації про їх логіку, значення та можливі наслідки для суб'єкта даних. Додатково, у праві ЄС ці положення функціонують у взаємозв'язку з новітніми регуляторними актами, зокрема EU AI Act [65], який запроваджує ризик-орієнтований підхід до використання систем штучного інтелекту, встановлює вимоги до прозорості, людського контролю та обмеження застосування високоризикових систем.

Натомість українське законодавство лише декларативно закріплює право особи знати про механізм автоматизованої обробки та право на захист від її наслідків, не визначаючи чітких критеріїв допустимості таких рішень, процедур їх оскарження та вимог до прозорості алгоритмів. Відсутність спеціального регулювання використання ШІ у сфері обробки

персональних даних формує нормативний вакуум, що стає особливо відчутним у контексті поширення технологій профілювання та автоматизованого прийняття рішень.

Не менш суттєві відмінності простежуються у сфері інституційного забезпечення контролю та нагляду за дотриманням законодавства про захист персональних даних. В ЄС функціонують незалежні наглядові органи (англ.: *data protection authorities*), наділені широким колом повноважень, зокрема щодо проведення перевірок, винесення обов'язкових для виконання приписів, а також застосування значних адміністративних санкцій. Ключовою ознакою їх діяльності є інституційна незалежність, що розглядається як фундаментальна гарантія ефективності системи захисту персональних даних та належного правозастосування. Натомість в Україні існуючий механізм нагляду не повною мірою відповідає зазначеним стандартам як за рівнем інституційної автономії уповноваженого органу, так і за обсягом наданих йому повноважень, що об'єктивно знижує ефективність реалізації та захисту відповідних прав.

Крім того, істотні розбіжності виявляються у підходах до встановлення юридичної відповідальності та застосування санкцій. GDPR запроваджує багаторівневу, диференційовану систему адміністративних штрафів, розмір яких може досягати значних сум і визначається з урахуванням характеру правопорушення, ступеня вини та інших релевантних обставин, що забезпечує їх реальний стримуючий ефект. Водночас у національному законодавстві України передбачені санкції є порівняно незначними та не здатні забезпечити належний рівень превенції, що, у свою чергу, сприяє формальному, а не змістовному дотриманню вимог законодавства у сфері захисту персональних даних.

Оперуючись вимогами Європейського Союзу у сфері захисту персональних даних стала підготовка і внесення до Верховної Ради України законопроєкту № 8153 «Про захист персональних даних» [13], зареєстрованого 25 жовтня 2022 року. Зазначений законопроєкт є спробою комплексного реформування національної моделі правового регулювання у сфері обробки персональних даних та її приведення у відповідність до сучасних міжнародних стандартів, передусім до положень GDPR [64] та модернізованої Конвенції 108+ [31].

Необхідність розроблення цього законопроєкту зумовлена тим, що чинне законодавство України у сфері захисту персональних даних не забезпечує належного рівня гарантій прав і свобод людини в умовах цифровізації. Закон України «Про захист

персональних даних» [8] 2010 року був сформований на основі підходів Директива 95/46/ЄС [43], яка на сьогодні втратила чинність і була замінена GDPR. Внаслідок цього українське регулювання істотно відстає від сучасних європейських стандартів, що проявляється у фрагментарності правового регулювання, відсутності чітких механізмів реалізації прав суб'єктів даних, а також недостатній визначеності обов'язків контролерів і операторів персональних даних.

20 листопада 2024 року Верховна Рада України ухвалила зазначений законопроєкт у першому читанні із доопрацюванням, що було позитивно оцінено європейськими експертними інституціями як важливий крок у напрямі гармонізації національного законодавства із правом ЄС. Станом на травень 2026 року законопроєкт перебуває на стадії підготовки до другого читання, що свідчить про його актуальність та складність узгодження окремих положень.

Змістовно законопроєкт № 8153 [13] передбачає глибоку трансформацію підходів до правового регулювання обробки персональних даних. Передусім, він істотно розширює перелік прав суб'єкта персональних даних, наближаючи їх до стандартів GDPR. Зокрема, вводяться такі ключові права, як «право бути забутим», право на обмеження обробки, право на перенесення даних, право на заперечення проти обробки, а також право не підлягати автоматизованому прийняттю рішень, що мають юридичні або подібні значущі наслідки.

Важливою новелою законопроєкту є запровадження принципів «*privacy by design*» та «*privacy by default»,* які передбачають інтеграцію вимог захисту персональних даних ще на етапі проєктування інформаційних систем та бізнес-процесів. Даний підхід суттєво змінює традиційну модель регулювання, переводячи акцент із реактивного контролю на превентивне забезпечення приватності.

Крім того, законопроєкт встановлює чіткі обов'язки контролерів і операторів персональних даних, зокрема щодо впровадження належних технічних та організаційних заходів захисту, ведення документації обробки даних, а також призначення відповідальної особи з питань захисту персональних даних. Значна увага приділяється також питанням прозорості обробки даних та інформування суб'єктів даних.

Окремо слід відзначити запровадження обов'язку повідомлення про порушення безпеки персональних даних протягом 72 годин з моменту виявлення такого порушення, що

відповідає вимогам GDPR [64] і спрямоване на мінімізацію негативних наслідків для суб'єктів даних.

Важливим положенням законопроєкту є посилення юридичної відповідальності за порушення законодавства у сфері захисту персональних даних шляхом запровадження ефективних і пропорційних санкцій.

Водночас затримка з остаточним ухваленням відповідного законопроєкту значною мірою зумовлена складністю інституційного реформування системи нагляду у сфері захисту персональних даних. Ключовим дискусійним питанням залишається модель майбутнього органу — чи має він функціонувати як колегіальний незалежний регулятор, чи як окрема спеціалізована служба. Вирішення цього питання є однією з принципових вимог ЄС у межах переговорного процесу щодо кластеру «Основи».

Практична реалізація гармонізації законодавства України з правом Європейського Союзу у сфері захисту персональних даних тісно пов'язана з процесами цифровізації державного управління та розширенням використання електронних сервісів. Показовим у цьому аспекті є функціонування державного цифрового сервісу «Дія», який забезпечує доступ до електронних документів, засобів електронної ідентифікації та публічних послуг. Його використання супроводжується системною обробкою значних обсягів персональних даних, що обумовлює підвищені вимоги до рівня їх правового захисту та відповідності європейським стандартам.

Україна у 2024–2025 роках також брала участь у пілотних проєктах ЄС щодо впровадження European Digital Identity Wallet (EUDI), що свідчить про поступову інтеграцію української цифрової інфраструктури до європейського цифрового простору та імплементацію принципів «*privacy by design*» [2]. Використання таких цифрових рішень супроводжується системною обробкою значних обсягів персональних даних, що зумовлює підвищені вимоги до рівня їх правового захисту та відповідності європейським стандартам.

Разом із тим розвиток таких цифрових інструментів виявляє певну невідповідність між динамікою технологічних змін та станом нормативно-правового регулювання. Чинне законодавство України у сфері захисту персональних даних не повною мірою відображає підходи, закріплені у праві ЄС, зокрема щодо забезпечення прозорості обробки даних,

реалізації принципу підзвітності та ефективності механізмів контролю за діяльністю суб'єктів, які здійснюють таку обробку. Особливої актуальності ці питання набувають в умовах воєнного стану, коли функціонування цифрових реєстрів, зокрема систем «Оберіг» і «Резерв+», пов'язане з використанням персональних даних як стратегічного ресурсу безпеки.

Водночас процес адаптації через гармонізацію законодавства України з правом Європейського Союзу стикається з низкою об'єктивних перешкод. Запровадження воєнного стану ускладнює повноцінне інституційне реформування, обмежує бюджетні ресурси та негативно впливає на адміністративну спроможність держави. Додатковими стримуючими чинниками виступають інституційна фрагментованість, дефіцит кваліфікованих кадрів у сфері захисту персональних даних, а також домінування технократичного підходу до цифровізації над належним урахуванням правового виміру захисту приватності.

Попри зазначені труднощі, перспективи гармонізації залишаються реалістичними за умови поетапного та послідовного впровадження відповідних реформ. Йдеться не лише про імплементацію європейських норм, а про формування нової правової культури захисту персональних даних, посилення інституційної спроможності органів контролю, інтеграцію принципів цифрової приватності у функціонування державних електронних сервісів, а також розвиток транскордонної співпраці у сфері кібербезпеки.

Отже, гармонізація законодавства України з правом Європейського Союзу у сфері захисту персональних даних і цифрової приватності виступає одним із ключових індикаторів готовності держави до членства в ЄС. Ефективність даного процесу визначає не лише рівень виконання євроінтеграційних зобов'язань, але й ступінь довіри громадян та європейських партнерів до функціонування української цифрової держави.

ВИСНОВКИ

Проведене дослідження міжнародно-правових механізмів захисту цифрової приватності та персональних даних засвідчило, що цифровізація суспільства спричинила якісну трансформацію однієї з базових гарантій прав людини — права на повагу до приватного життя.

Інтенсивний розвиток інформаційно-комунікаційних технологій, глобалізація обробки даних, а також поширення штучного інтелекту сформували нові виклики, що потребують перегляду традиційних підходів до забезпечення приватності.

Цифрова приватність у сучасному міжнародному праві функціонує як результат еволюції класичного права на приватне життя, доповнений специфічними механізмами захисту в умовах обробки великих масивів даних та транскордонних інформаційних потоків. Вона набуває міжгалузевого характеру, поєднуючи елементи права прав людини, кібербезпеки та регулювання цифрової економіки.

Актуальний етап розвитку міжнародного права характеризується зміною парадигми захисту приватності: від моделі, спрямованої виключно на обмеження державного втручання, до комплексної системи, яка охоплює як діяльність державних органів, так і вплив приватних суб'єктів, зокрема глобальних технологічних компаній. Така трансформація зумовлює закріплення позитивних зобов'язань держав щодо створення ефективних правових, інституційних та технічних гарантій захисту особи у цифровому середовищі.

Суттєвою ознакою сучасного правового регулювання є також поступовий перехід від актів рекомендаційного характеру до формування юридично обов'язкових міжнародних стандартів. Прийняття новітніх міжнародно-правових інструментів, зокрема у сфері штучного інтелекту, свідчить про прагнення міжнародної спільноти встановити чіткі межі допустимого застосування цифрових технологій з урахуванням необхідності забезпечення та захисту прав людини.

У межах першого розділу було обґрунтовано, що право на повагу до приватного життя є основоположною категорією, яка забезпечує формування системи міжнародно-правового захисту цифрової приватності. Еволюція права — від класичних доктринальних підходів до

сучасних нормативних стандартів — засвідчує поступове розширення його змісту до охоплення інформаційного та цифрового вимірів особистості.

Історичний розвиток міжнародно-правових гарантій підтверджує, що універсальні акти, зокрема Загальна декларація прав людини [75] та Міжнародний пакт про громадянські і політичні права [56], заклали фундаментальні принципи захисту приватності. Їх подальша конкретизація відбувалася в межах регіональних систем та міжнародних інституцій, що сприяло формуванню більш деталізованого правового режиму захисту персональних даних.

Важливим результатом стало те, що сучасна доктрина розвиває розуміння приватності через категорію «*цифрових прав*», яка охоплює новітні аспекти взаємодії особи з цифровим середовищем. Міжнародні акти, прийняті в межах Організації Об'єднаних Націй, підкреслюють необхідність забезпечення державами не лише невтручання, а й активного захисту від зловживань з боку приватних суб'єктів.

Аналіз впливу технологій штучного інтелекту дозволив виявити нові системні ризики для приватності, які проявляються через автоматизоване профілювання, масове накопичення персональних даних та використання біометричних технологій. Реакцією на ці виклики стало формування нових міжнародних підходів до регулювання, що передбачають посилення контролю, оцінку ризиків та підзвітність суб'єктів, які застосовують такі технології.

Результати другого розділу засвідчили, що міжнародно-правові механізми захисту цифрової приватності формуються як багаторівнева система, у межах якої універсальні норми визначають загальні орієнтири, а регіональні механізми забезпечують їх ефективну реалізацію.

Універсальна система міжнародного права, представлена актами ООН, відіграє важливу роль у формуванні загальних стандартів, однак її ефективність обмежується відсутністю дієвих механізмів примусу та високим рівнем абстрактності нормативних приписів. Водночас ці акти виконують функцію нормативної основи для подальшого розвитку більш деталізованих правових режимів.

Європейська модель захисту персональних даних є найбільш розвиненою та інституційно забезпеченою. Загальний регламент про захист даних сформував цілісну систему правового регулювання, яка поєднує права суб'єктів даних з обов'язками

контролерів і процесорів, а також передбачає наявність незалежних наглядових органів та ефективних санкцій.

Важливою особливістю сучасного етапу є запровадження функціонального підходу до визначення юрисдикції, який відображений в екстериторіальній дії GDPR. Така модель дозволяє поширювати правовий захист на осіб незалежно від місця обробки їхніх персональних даних та сприяє глобалізації європейських стандартів.

Практика Європейського суду з прав людини відіграє ключову роль у конкретизації змісту права на приватність. Суд розширив сферу застосування статті 8 ЄКПЛ [46], включивши до неї цифрові аспекти існування особи, та сформував чіткі критерії оцінки допустимості втручання у приватне життя.

Сформовані підходи мають визначальне значення для розуміння меж застосування технологій масового спостереження та обробки персональних даних.

Окремої уваги потребує вплив цифрових технологій на інші права людини. Наявність потенційного контролю за поведінкою особи у цифровому середовищі може призводити до самообмеження у реалізації свободи вираження поглядів і свободи зібрань, що підтверджує міжгалузевий характер проблеми цифрової приватності.

Дослідження, здійснене у третьому розділі, показало, що Україна перебуває на етапі активного реформування національної системи захисту персональних даних у напрямі її гармонізації з європейськими стандартами. Конституційні гарантії створюють належну правову основу, однак чинне законодавство потребує подальшого вдосконалення з урахуванням сучасних вимог.

Ключовим завданням залишається імплементація положень GDPR [64] та формування ефективної інституційної системи контролю. Особливої уваги потребує створення незалежного наглядового органу, який відповідатиме європейським критеріям ефективності, незалежності та підзвітності.

Складність реалізації реформ зумовлена як інституційними, так і об’єктивними факторами, пов’язаними з умовами воєнного стану. Забезпечення балансу між інтересами національної безпеки та захистом права на приватність набуває особливої ваги в умовах підвищених кіберзагроз та необхідності обробки значних обсягів персональних даних.

Узагальнюючи результати дослідження, можна зробити висновок, що сучасна система міжнародно-правового захисту цифрової приватності перебуває у стані динамічного розвитку та характеризується поступовим переходом до комплексної моделі регулювання. Вона поєднує елементи міжнародного права прав людини, регулювання цифрових технологій та механізмів кібербезпеки, формуючи нову правову реальність.

Ключовою тенденцією сучасного етапу розвитку міжнародно-правового регулювання у сфері цифрової приватності є поєднання трьох взаємопов'язаних напрямів: посилення нормативного регулювання шляхом формування юридично обов'язкових міжнародних стандартів («жорсткого права»), розвиток інституційних механізмів контролю та нагляду, а також впровадження превентивних технічних підходів до захисту персональних даних і приватності. Усе більшого значення набувають принципи «*privacy by design*» та «*privacy by default*», які орієнтують держави й суб'єктів цифрової економіки на інтеграцію гарантій захисту прав людини безпосередньо у процес створення та функціонування цифрових технологій.

За таких умов цифрова приватність поступово перетворюється на один із ключових елементів сучасної архітектури прав людини та невід'ємну складову демократичного правопорядку. Її забезпечення виходить за межі виключно інформаційно-правового регулювання та охоплює питання кібербезпеки, функціонування цифрових платформ, розвитку штучного інтелекту, транскордонної передачі даних і гарантування інформаційної автономії особи. Саме тому рівень захисту цифрової приватності дедалі більше визначає ступінь демократичності держави, ефективність функціонування її правових інститутів та відповідність сучасним міжнародним стандартам у сфері прав людини

Підсумовуючи результати проведеного дослідження, слід зазначити, що ефективний захист цифрової приватності можливий лише за умови застосування комплексного та міждисциплінарного підходу, що передбачає узгодження міжнародних стандартів, національного законодавства та сучасних технологічних практик. Водночас необхідною умовою залишається забезпечення справедливого балансу між розвитком цифрових інновацій, інтересами державної безпеки, економічними потребами цифрового ринку та належним захистом фундаментальних прав і свобод людини. У перспективі подальший розвиток міжнародного права у цій сфері буде спрямований на формування універсальних

механізмів відповідальності та контролю за використанням цифрових технологій, здатних гарантувати збереження людської автономії, гідності та приватності в умовах глобальної цифрової трансформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ваганова І. Зобов'язання, що виникають із деліктів у Римському праві. Актуальні питання у сучасній науці. 2024. № 3(21). URL: https://doi.org/10.52058/2786-6300-2024-3(21)-510-521

2. Європейський цифровий гаманець ініціатива Європарламенту. Міністерство цифрової трансформації України. URL: https://thedigital.gov.ua/news/technologies/evroparlament-pidtrimav-rozrobku-evropeyskogo-tsifrovogo-gamantsya

3. Кодекс України про адміністративні правопорушення : Кодекс України від 07 грудня 1984 р. № 8073-X. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/8073-10#top

4. Конституція України : від 28.06.1996 № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

5. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III : станом на 15 квіт. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

6. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022 : станом на 1 трав. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text

7. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI : станом на 8 серп. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text

8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

9. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 20 січ. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

10. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 19 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

11. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Закон України від 16.09.2014 № 1678-VII. URL: https://zakon.rada.gov.ua/laws/show/1678-18#Text (дата звернення: 07.05.2026).

12. Про Уповноваженого Верховної Ради України з прав людини : Закон України від 23.12.1997 № 776/97-ВР : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/776/97-вр#Text

13. Проєкт Закону про захист персональних даних № 8153 від 25 жовтня 2022 р. Верховна Рада України. URL: https://itd.rada.gov.ua/billinfo/Bills/Card/40707

14. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : Рішення Конституц. Суду України від 20.01.2012 № 2-рп/2012. URL: https://zakon.rada.gov.ua/laws/show/v002p710-12#Text

15. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України "Про інформацію" та статті 12 Закону України "Про прокуратуру" (справа К.Г.Устименка) : Рішення Конституц. Суду України від 30.10.1997 № 5-зп. URL: https://zakon.rada.gov.ua/laws/show/v005p710-97#Text

16. Сполучення слів з Data Privacy. Cambridge Dictionary. English Dictionary, Translations & Thesaurus. URL: https://dictionary.cambridge.org/uk/example/english/data-privacy.

17. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014 : станом на 14 жовт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

18. Харитонов Є, Тищук Н. Формування деліктів римського права як прототипу сучасної системи диференціації правопорушень. 2018. № 27. ст. 9-14. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/66fabb54-192c-4782-85f5-ca4598295c50/content

19. Цивільний кодекс України : Кодекс України від 16.01.2003 № 435-IV : станом на 1 лют. 2026 р. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text

20. Яким'юк С. М. Захист персональних даних в умовах воєнного стану в Україні: виклики цифрової безпеки та міжнародні стандарти. Права людини в умовах воєнного стану в Україні : матеріали Всеукраїнської науково-практичної конференції (XI Круглого столу). Київ : Київський столичний університет імені Бориса Грінченка, 2025. URL: https://kubg.edu.ua/images/phocagallery/astrea/2025/12_12_prava-liudyny-v-umovakh-voiennoho-stanu/Prohrama_Kruhlyi_stil_2025.pdf

21. Яким'юк С. М. Захист права на приватність у цифровому середовищі: аналіз практики ЄСПЛ. Міжнародне та публічне право: перспективи та виклики : матеріали III студентської наукової конференції. Київ : Київський столичний університет імені Бориса Грінченка, 2026. URL: https://fpmv.kubg.edu.ua/images/stories/Departaments/1_kmpeei/Naukovi_zaxodu/Prohrama_stud_konf_2026.pdf

22. African Charter on Human and Peoples' Rights. Organization of African Unity. 1981. URL: https://www.oas.org/en/sla/dil/docs/African_Charter_Human_Peoples_Rights.pdf

23. AI Act vs GDPR: Differences, Overlap Areas and Implications for Your Organisation. AiActo. URL: https://www.aiacto.eu/en/blog/ai-act-rgpd-differences-complementarites

24. American Convention on Human Rights. Organization of American States.1969. URL: https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.pdf

25. Arab Charter on Human Rights (revised). League of Arab States. 2004. URL: https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/Revised_Arab_Charter_Human_Rights_2004_Em.pdf

26. Bărbulescu v. Romania [GC], no. 61496/08, Judgment of the European Court of Human Rights, 5 September 2017. HUDOC. URL: https://hudoc.echr.coe.int/fre?i=001-177082

27. Big Brother Watch and Others v. the United Kingdom [GC], judgment of the European Court of Human Rights of 25 May 2021, applications nos. 58170/13, 62322/14 and 24960/15. HUDOC. URL: https://hudoc.echr.coe.int/fre?i=001-210077

28. Bradford A. The Brussels Effect: How the European Union Rules the World. Oxford University Press, 2020. URL: https://global.oup.com/academic/product/the-brussels-effect-9780190088583?cc=ua&lang=en&

29. CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. UN Human Rights Committee. 1988. URL: https://www.refworld.org/legal/general/hrc/1988/27539.

30. Charter of Fundamental Rights of the European Union. European Union. 2012. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT.

31. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe. 1981. URL: https://rm.coe.int/1680078b37.

32. Convention on Cyber Security and Personal Data Protection. African Union. 2014. URL: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

33. Convention on Cybercrime. Council of Europe. 2001. URL: https://rm.coe.int/1680081561.

34. Convention on the Rights of Persons with Disabilities. United Nations. 2006. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities.

35. Convention on the Rights of the Child. United Nations. 1989. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child.

36. Convention Relating to the Status of Refugees. United Nations. 1951. URL: https://www.unhcr.org/media/1951-refugee-convention-and-1967-protocol-relating-status-refugees.

37. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, CETS No. 225, Strasbourg, 17 May 2024. Council of Europe. URL: https://rm.coe.int/1680afae3c

38. Cyber Dimensions of the Armed Conflict in Ukraine. Geneva : CyberPeace Institute, 2023. URL: https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf

39. Data Protection Act 1998. London, United Kingdom. 1998. URL: https://www.legislation.gov.uk/ukpga/1998/29/contents.

40. Data Protection Act 2018. United Kingdom. 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents

41. Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems ("Schrems II"), Case C-311/18, Judgment of the Court of Justice of the European Union, 16 July 2020. CURIA. URL: https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-311%2F18%22&publishedId=C-311%2F18

42. Digital Personal Data Protection Act, 2023 : Act No. 22 of 2023 of 11 August 2023. India. URL: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

43. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. European Parliament and Council of the European Union. 1995. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

44. Duguin S., Pavlova P. The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict. European Parliament. 2023. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf

45. Dul C. Facial Recognition Technology vs Privacy: The Case of Clearview AI. Queen Mary Law Journal. 2022. Vol. 3. P. 1–24. URL:

https://www.qmul.ac.uk/law/research/journals/the-queen-mary-law-journal/media/law/docs/research/2022QMLJ1.pdf

46. European Convention on Human Rights. Council of Europe. 1950. URL: https://www.echr.coe.int/documents/d/echr/convention_ukr.

47. Facial recognition: Italian SA fines Clearview AI EUR 20 million. Garante per la protezione dei dati personali. URL: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9751362

48. Gaughran v. the United Kingdom, no. 45245/15, Judgment of the European Court of Human Rights, 13 February 2020. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-200817

49. General comment no. 34, Article 19, Freedoms of opinion and expression. UN Human Rights Committee. 2011. URL: https://www.refworld.org/legal/general/hrc/2011/83764.

50. General Personal Data Protection Law (LGPD) : Law No. 13.709 of 14 August 2018. Brazil. URL: https://www.lgpdbrasil.com.br/wp-content/uploads/2019/06/LGPD-english-version.pdf

51. Glukhin v. Russia, no. 11519/20, Judgment of the European Court of Human Rights, 4 July 2023. HUDOC. URL: https://hudoc.echr.coe.int/?i=001-225655

52. Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data. Organisation for Economic Cooperation and Development. 1980. URL: https://www.refworld.org/policy/legalguidance/oecd/1980/14534.

53. History of the Cambridge Analytica Controversy. Bipartisan Policy Center. URL: https://bipartisanpolicy.org/article/cambridge-analytica-controversy/.

54. Inter-American Principles on Personal Data Protection. Organization of American States. 2015. URL: https://www.oas.org/en/sla/dil/docs/CJI-doc_474-15_rev2.pdf

55. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families. United Nations. 1990. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-protection-rights-all-migrant-workers.

56. International Covenant on Civil and Political Rights. United Nations. 1966. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

57. M.M. v. the United Kingdom, no. 24029/07, Judgment of the European Court of Human Rights, 13 November 2012. HUDOC. URL: https://hudoc.echr.coe.int/eng?i=001-114517

58. Mandate of the Special Rapporteur on the right to privacy. Office of the United Nations High Commissioner for Human Rights. URL: https://www.ohchr.org/en/special-procedures/sr-privacy

59. Maximillian Schrems v Data Protection Commissioner, Case C-362/14, Judgment of the Court of Justice of the European Union, 6 October 2015. CURIA. URL: https://infocuria.curia.europa.eu/tabs/affair?sort=AFF_NUM-DESC&searchTerm=%22C-362%2F14%22&publishedId=C-362%2F14&lang=EN

60. Meta Ireland fined €1.2 billion by Irish Data Protection Commission. European Data Protection Board. URL: https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_lv

61. Meta Platforms Inc. and Others v Bundeskartellamt (Case C-252/21), Judgment of 4 July 2023. Court of Justice of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A62021CJ0252

62. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223, Strasbourg, 10 October 2018. Council of Europe. URL: https://rm.coe.int/16808ac918

63. R (Bridges) v Chief Constable of South Wales Police. Judgment of 11 August 2020. Court of Appeal (England and Wales). URL: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf

64. Regulation (EU) 2016/679 (General Data Protection Regulation). European Parliament and Council of the European Union. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

65. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj?

66. Reservations and Declarations for Treaty No. 005 – Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005). Council of Europe Treaty Office. URL: https://www.coe.int/en/web/Conventions/full-list/?module=declarations-by-treaty&numSte=005&codeNature=10&codePays=U

67. Russia's war on Ukraine: Timeline of cyber-attacks. European Parliament Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI%282022%29733549_EN.pdf

68. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland [GC], no. 931/13, Judgment of the European Court of Human Rights, 27 June 2017. HUDOC. URL: https://hudoc.echr.coe.int/fre?i=001-175121

69. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Council of Europe. 2022. URL: https://rm.coe.int/1680a49dab.

70. State Service of Special Communications and Information Protection of Ukraine, CERT-UA. Russia's Cyber Tactics H1'2023. Kyiv, 2023. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=60068

71. The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC. European Data Protection Board. URL: https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_ga

72. Treaty on the Functioning of the European Union (consolidated version). Official Journal of the European Union. 2016. C 202. P. 47–390. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12016E%2FTXT&um

73. Ukraine. Enlargement and Eastern Neighbourhood. URL: https://enlargement.ec.europa.eu/countries/ukraine_en.

74. United Nations General Assembly. *The right to privacy in the digital age* : resolution adopted by the General Assembly, A/RES/79/175, 19 December 2024. URL: https://digitallibrary.un.org/record/4071978?ln=en&v=pdf

75. Universal Declaration of Human Rights. United Nations. 1948. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

76. Warren S. D., Brandeis L. D. Right to Privacy. Harvard Law Review. 1890. URL: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

77. Westin A. F. Privacy and Freedom. Washington and Lee Law Review. 1968. Vol. 25, No. 1. 166 ст. URL: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20

ДОДАТКИ

Додаток А

Статистичні дані щодо найбільших індивідуальних штрафів у сфері захисту персональних даних відповідно до GDPR (Топ-10)

	Controller	Sector	Country	Fine [€]	Type of Violation	Date
1	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	1200000000	Insufficient legal basis for data processing	2023-05-12
2	TikTok Technology Limited	Media, Telecoms and Broadcasting	IRELAND	530000000	Insufficient legal basis for data processing	2025-05-02
3	Meta Platforms, Inc.	Media, Telecoms and Broadcasting	IRELAND	405000000	Non-compliance with general data processing principles	2022-09-05
4	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	390000000	Non-compliance with general data processing principles	2023-01-04
5	TikTok Limited	Media, Telecoms and Broadcasting	IRELAND	345000000	Non-compliance with general data processing principles	2023-09-01
6	LinkedIn	Media, Telecoms and Broadcasting	IRELAND	310000000	Insufficient legal basis for data processing	2024-10-24
7	Uber Technologies Inc., Uber B.V.	Employment	THE NETHERLANDS	290000000	Non-compliance with general data processing principles	2024-07-22
8	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	265000000	Insufficient technical and organisational measures to ensure information security	2022-11-25
9	Meta Platforms Ireland Limited	Media, Telecoms and Broadcasting	IRELAND	251000000	Insufficient technical and organisational measures to ensure information security	2024-12-17
10	WhatsApp Ireland Ltd.	Media, Telecoms and Broadcasting	IRELAND	225000000	Insufficient fulfilment of information obligations	2021-09-02

Джерело: Statistics: Highest individual fines (Top 10). GDPR Enforcement Tracker. URL: https://www.enforcementtracker.com/?insights=&performance=