

УДК 342.7

ГЕНЕЗА ПРАВОВОГО ЗАХИСТУ ПРИВАТНОСТІ ОСОБИ

Віталій Чорненький

*Львівський національний університет імені Івана Франка,
вул. Університетська, 1, Львів, Україна, 79000
e-mail: vitaliy.chornenkyu@lnu.edu.ua
ORCID ID: 0000-0001-5067-0844*

Проведено системне дослідження становлення і розвитку правового захисту приватності особи від античних і середньовічних форм до сучасного конституційно-правового режиму. Реконструйовано еволюцію поняття приватності як правової категорії, простежуючи її шлях від процедурних звичаїв і станових привілеїв до універсального права людини. З'ясовано, що ще в римському праві через інститути *dominium* та *domus* було закладено базові контури приватної сфери, а середньовічні режими «домашнього миру», корпоративних таємниць і канонічного *forum internum* створили перші правові обмеження доступу до особистого простору.

Показано, що модерна доба принесла перехід від фактичних бар'єрів до конституційних гарантій: рішення *Semayne's Case* (1604), *Entick v. Carrington* (1765) і стаття Воррена та Брандейса (1890) започаткували правове осмислення приватності як самостійного об'єкта охорони. Автор доводить, що ХХ ст. сформувало міжнародно-правовий фундамент цього права – від ст. 12 Загальної декларації прав людини до ст. 8 Європейської конвенції – і забезпечило його конкретизацію через практику ЄСПЛ та Суду ЄС.

На основі порівняльного аналізу англо-американської та континентальної правових систем у статті виявлено відмінності підходів до регулювання приватності: перша базується на процедурних стримуваннях влади, друга – на гідності та інформаційному самовизначенні особи. В роботі запропоновано авторську модель конституційно-правового режиму приватності, що складається з трьох груп принципів: матеріально-правових (законність, легітимна мета, «якість закону»), процедурно-правових (необхідність, пропорційність, незалежний нагляд) та інституційних (підзвітність і ефективні засоби захисту).

З'ясовано, що українська модель охорони приватної сфери, спираючись на ст. 30-32 Конституції України, поступово гармонізується з європейськими стандартами, виробленими ЄСПЛ і Судом ЄС, однак потребує подальшої імплементації запобіжників щодо судового контролю, зберігання даних і повідомлення особи про втручання. Отож у статті вперше комплексно узагальнено історичні витоки, структурні принципи та сучасні виклики правового захисту приватності, що становить внесок у формування національної доктрини у цій сфері.

Ключові слова: автономія особи; гідність; пропорційність; контроль; персональні дані.

DOI: <http://dx.doi.org/10.30970/vla.2025.81.146>

Вступ. Стрімкий розвиток інформаційно-комунікаційних технологій, систем масового спостереження та збору персональних даних створюють принципово нові запити до правового регулювання. Останнє визначає потребу в переосмисленні класичних підходів до розуміння приватної сфери індивіда та вироблення адекватних правових механізмів її захисту, які б враховували специфіку сьогодення. В Україні особливої гостроти набуває проблема збалансування захисту приватної сфери із потребами національної безпеки. Все це ставить перед науковою спільнотою завдання сформулювати таку правову конструкцію захисту приватності особи,

котра була б водночас і доволі гнучкою, аби бути здатною для функціонування у динамічному середовищі, а з іншого – доволі надійною та ефективною.

Зі свого боку, розуміння сучасних правових інститутів неможливе без з'ясування їх історичного походження та еволюції. Генетичний аналіз дозволяє виявити глибинні закономірності формування концепції приватності, простежити, як соціально-політичні зміни впливали на зміст та обсяг правової охорони приватної сфери особи. Це особливо важливо для приватності, оскільки це поняття не є статичним – воно постійно трансформується під впливом технологічних, соціальних та політичних факторів.

Тим чи іншим аспектам охарактеризованої проблеми присвячено праці Семюела Д. Воррена, Луїса Д. Брандейса, Вільяма Проссера, Деніела Солова, Гелен Ніссенбаум, Джулі Коен, Джеймса Вітмана, Аніти Аллен, Віктора Майєр-Шенбергера, Алана Вестіна, Ніла Річардса, Райана Карло, Хелен Андерсон, Данієль Цитрон, С. В. Різника, О. М. Бориславської, В. Ф. Погорілка, М. І. Козюбри, М. В. Савчина, А. О. Селіванова, В. В. Городовенка, П. Б. Євграфова, А. А. Єзерова, А. р. Крусян, В. В. Лемака, О. М. Литвинова, С. Б. Булеци, М. Ю. Віхляєва, М. В. Громовчук, Л. М. Дешко. Запропонований нижче матеріал становить спробу водночас об'єднати та поглибити наявні знання в окресленій проблематиці.

Мета запропонованої статті – реконструювати еволюцію правового захисту приватності особи від римського права до сучасних правопорядків держав континентального та загального права, а також показати, як новітні загрози (політичні, технологічні, соціальні) детермінують зміни змісту та обсягу її юридичної охорони, захисту та забезпечення.

Виклад основного матеріалу. Термін «приватний» в індо-європейській мовній сім'ї історично артикулював насамперед межу між «своїм» і «спільним» чи «загальним», що добре простежується на матеріалі класичних мов і новосередньовісних традицій. Так, лат. *privatus* означає «вилучений із державної сфери», «той, хто не обіймає публічної посади», і безпосередньо пов'язаний із дієсловом *privare* – «позбавляти, відділяти», отже, первинним є мотив відмежування і недопуску [71; 72]. Давньогрег. *ἰδιος* («власний, свій») дало *ιδιότης* – «приватна особа», тобто не посадовець, що підкреслює розрізнення «власного» та «публічного» [73]. В англійській *privacy* історично контрастує з *public* і семантично межує з *privation* *to deprive* (лінія від лат. *privare*), тож акцент падає на контролі доступу і можливості «утримувати осторонь», «не допускати» [74; 75; 76]. Натомість у французькій традиції закріпився вираз *vie privée* – буквально «приватне життя», який радше акцентує зміст життя поза публічною сферою; звідси й усталена правова формула *droit au respect de la vie privée* («право на повагу до приватного життя») у ст. 9 *Code civil* [77; 78]. Уже з цієї мовної карти випливає елементарне ядро: приватність – це насамперед про межу (просторову, комунікаційну, інформаційну) і про владу над доступом крізь цю межу.

Античні та середньовічні витoki приватності: «не-публічність» як правопорядок простору. Римське право запровадило основні «контури» приватної сфери через регулювання інститутів *dominium* та *domus*: недоторканність приватної власності, автономія домовладки, деліктна охорона честі й гідності – усе це, хоч і без сучасних правових категорій, сформувало простір, куди публічна влада отримувала доступ лише через, так би мовити, спеціальні «процесуальні шлюзи» (як-от, у формі позовів, притягнення до відповідальності за делікти проти особи та майна тощо). Середньовічна рецепція римського права (з відповідною канонічною корекцією) посилила ідею внутрішнього виміру свободи – *forum internum* – як сфери,

що не підлягає примусу. Водночас політична структура феодальних юрисдикцій розкладала «приватність» на територіальні та станові сегменти: звичаєві правила входу до житла, локальні привілеї, таємниці цехів і міських комун.

Цікаво, що у феодальних володіннях діяли власні судові й поліцейські режими (маноріальні й доменіальні юрисдикції, міські комуни, церковні вотчини), які встановлювали правила доступу до помешкання підданого. Ключовим був звичай «домашнього миру» (*Hausfrieden* – охорона спокою домогосподарства): без санкції місцевої влади або без законної причини (переслідування злочинця, гасіння пожежі, рятування) сторонній – включно з представником сюзерена – не мав права входити до житла. Порушення тягло локально визначені санкції як за посягання на мир громади. Водночас, залежно від міського права (типу магдебурзького чи любецького), вхід державця чи посадовця, зазвичай, вимагав присутності свідків або «добрих людей» громади та дотримання денного часу; нічний обшук заборонявся або допускався лише у вузько визначених випадках [56]. Тобто «правила дверей» були частиною поліційно-правового порядку міста чи маєтку, а не індивідуального суб'єктивного права власника в сучасному розумінні.

У королівствах і князівствах існував пласт «іmunітетів» (англ. *immunities*, лат. *immunitas*), коли король передавав власну судово-поліцейську компетенцію світським або духовним феодалам. Усередині таких «іmunітетних округів» діяв автономний порядок входу до житла, обшуку й виїмки, який відрізнявся від загальнодержавного. Тож, як можна простежити, *приватність «розкладалася» територіально*: один і той самий підданий мав різний обсяг фактичного захисту залежно від того, чи перебував він у межах міста з широкою комунальною свободою, у графському домені або в церковній сеньйорії. Відповідно, інструменти протидії свавільному вторгненню були процедурними (вимога участі старшин громади, денного часу, попередження), а не правами в сенсі «недоторканності житла» як конституційної гарантії (яка з'явиться значно пізніше) [29].

Станова структура (англ. *estates*) породжувала різні «ранги» приватності. Дворянська оселя, клерикальна резиденція чи купецький дім у привілейованому боро мали в середньовічній Європі вищий рівень фактичних бар'єрів для вторгнення ніж селянська хижка поза міською стіною. Привілеї міст (хартії) закріплювали обмеження для королівських агентів: наприклад, заборону нічних вторгнень, вимогу попереднього виклику господаря, участі присяжних тощо. Ці обмеження, утім, «переламувалися» загальнокоролівськими обов'язками – *hue and cry* (переслідування злочинця всією громадою), *watch and ward* (нічні варти), комендантською годиною, коли доступ до будинків дозволявся для дотримання публічного порядку. Саме на цьому тлі англійська доктрина «дім – фортеця» отримує своє класичне формулювання у *Semayne's Case* (1604), але її соціально-правові передумови накопичувалися у міських і маноріальних звичаях попередніх століть [30].

Цікаво, що інформаційна «приватність» на середньовічному вимірі існувала переважно як корпоративна таємниця, закріплена в конкретних нормативних актах. Статути флорентійської гільдії *Arte della Lana* (1317–1319) встановлювали суворі зобов'язання щодо нерозголошення технологічних секретів шерстяного виробництва, включаючи рецептури фарбування та обробки тканин. Венеційський статут про промислові привілеї 1474 р. прямо передбачав захист «секретності оатів» (*secrecy oaths*) для майстрів, які передавали знання через учнівство [Commentary on: Venetian Statute on Industrial Brevets (1474)]. Лондонські цехові хартії XIII–XIV ст. містили положення про заборону розголошення «таємниць ремесла» під загрозою виключення з гільдії та штрафних санкцій [57]. Аналогічно німецькі міські комуни

у своїх статутах (зокрема, в містах із магдебурзьким правом) встановлювали режим «секретів міста» (*Stadtgeheimnisse*) – оборонних, фінансових, митних відомостей, до яких доступ мали лише члени міської ради та окремі посадовці. І знову ж – це не індивідуальне право на дані, а правовий режим корпоративної конфіденційності, який випереджав сучасні категорії торговельної таємниці і персональних даних.

Для належного розуміння змісту і обсягу сучасної правової охорони приватності варто брати до уваги канонічний вимір проблематики: «внутрішня сфера» (*forum internum*) і печать сповіді створювали, мабуть, найсильніший тогочасний бар'єр проти розкриття відомостей про особу. Але цей бар'єр носив радше сакрально-інституційний (церковна заборона і відповідні санкції), а не був правом у сенсі публічно-правових вимог до держави та її посадових осіб. Утім, канонічні уявлення про внутрішню автономію згодом живитимуть модерні доктрини свободи сумління й приватного життя.

Тож, як бачимо, «приватність» у середньовічній Європі має форму строкатої мозаїки правопорядків і привілеїв: територіальні режими доступу до житла, станові асиметрії, корпоративні таємниці і сакральні заборони. Їх поєднували, очевидно, дві риси – процедурність і локальність, – і саме з цього, зрештою, виросте модерна процесуальна доктрина обмежень на порушення недоторканності житла й кореспонденції, яка, після конституційних переломів раннього модерну, буде кодифікована у великих хартіях і прецедентах загального права, а згодом у конституціях та законах [29, 30, 31].

Кристалізація юридично значущих меж між «публічним» і «приватним» на зламі середньовіччя і модерну відбулася, так чи інакше, через конституційні обмеження влади. *Magna Carta* закріпила ранні гарантії від свавільних вторгнень, започаткувавши традицію процесуальних стримувань (*due process*) для будь-якого втручання у приватну сферу [29].

Далі англійське загальне право деталізувало недоторканність житла: у справі *Semayne's Case* (1604) суд вивів обов'язок попередження («*knock-and-announce*») як елемент законності проникнення [30], а в *Entick v. Carrington* (1765) встановлено принципову заборону «загальних ордерів» та вимогу чіткої правової підстави для обшуку й вилучення [31]. Паралельно сформувались і контури захисту конфіденційності, що видно з таких справ, як *Prince Albert v. Strange* (1849), де превентивний засіб (судова заборона – англ. *injunction* – запобіжний інструмент) дозволив заборонити публікацію приватних зображень [32]. Усі ці норми й рішення, хоча й адресували різні об'єкти (житло, папери, зображення), поступово вибудовували єдину логіку: приватна сфера є юридичною категорією, а не лише соціальним фактом.

Слід наголосити, що ранні компроміси між «зовнішньою» лояльністю та «внутрішньою» свободою (насамперед у сфері віросповідання) дали поштовх нинішньому розумінню автономії переконань як складника приватного життя. Ця дихотомія, хоча і не була сформульована мовою основних прав, екстраполювалася згодом на таємницю листування, професійної діяльності та інформаційні відносини, що чітко простежується у подальшій прецедентній і міжнародній еволюції [1–3; 15–18].

Модерний злам (XVI–XIX ст.): держава, технології та індивідуальна автономія. Модерна держава, централізуючи публічну владу, одночасно змушена була визначити свої межі втручання у житло та кореспонденцію громадян. Цей процес рухався двома шляхами. По-перше, через посилення процесуальних гарантій у загальному праві – від заборони «загальних ордерів» до вимоги судового контролю й визначеності підстав втручання [30–31]. По-друге, через технологічні інновації, які висунули нові об'єкти охорони.

Так, поява розвиненої поштової служби спричинила конституційну доктриналізацію таємниці кореспонденції у США: рішення у справі *Ex parte Jackson* (1878) прирівняло поштові відправлення до «паперів» у значенні заборони необґрунтованих обшуків і вилучень [33], а *Boyd v. United States* (1886) пов'язала цю заборону з принципом неприпустимості примусового самовикриття, захищаючи приватні документи від використання державою поза межами належної процедури [34]. В англійській традиції доктрина *equity* надавала превентивний захист конфіденційній інформації, що набуло наступного розвитку в прецедентах деліктної сфери.

Важливо наголосити, що саме цей модерний період (умовно – від Реформації до другої індустріальної революції) забезпечив матеріал для пізнішої конституціоналізації приватності в міжнародних актах XX ст. та в юриспруденції прав людини [1–3]. Тобто процесуальні формули, вироблені загальним правом, і матеріальні режими захисту інформації (зображень, паперів, кореспонденції) створили «юридичний інвентар», без якого не існувало би ані сучасних критеріїв порушення ст. 8 ЄКПЛ, ані сучасних стандартів захисту даних.

Публікація Семюеля Воррена та Луїса Брандейса «The Right to Privacy» (1890) справила потужний вплив на концептуалізацію предмета нашого дослідження, позаяк приватність була концептуалізована як самостійний об'єкт охорони, відмежований від наклепу та деліктів власності, з акцентом на превентивні засоби захисту (англ. *injunction* – судова заборона) [55]. Подальша американська доктрина (зокрема, систематизація Проссера) виокремила чотири типи посягань: порушення усамітнення (англ. *intrusion upon seclusion*), привласнення імені/зображення (англ. *appropriation*), оприлюднення приватних фактів (англ. *public disclosure of private facts*), подання особи в хибному світлі (англ. *false light*) [56]. Хоча це – приватно-правова площина, саме вона створила зручні «формати» і для публічно-правових міркувань про обсяг і зміст охорони й захисту приватної сфери.

Паралельно з деліктною систематикою в США відкрилася конституційна траєкторія: «зони приватності» у *Griswold v. Connecticut* (1965) [35], відмова від суто територіальної логіки через критерії «обґрунтованого очікування приватності» у *Katz v. United States* (1967) [36], подальше розгортання інформаційної приватності у справах *Whalen v. Roe* [37], *Smith v. Maryland* [38], а вже в цифрову добу – у *Riley v. California* [39] і *Carpenter v. United States* [40]. Для нашого дослідження це означає, що *приватність стала універсальною координатою і в приватноправових, і в публічно-правових спорах; змінився лише інструментарій захисту*.

XX століття: тоталітарні виклики та конституціоналізація. Історія XX ст. – це, по суті, рух від «негативних» заборон втручання до «позитивних» обов'язків держави створити режимну (конституційно й законодавчо) охорону приватного життя. Міжнародні акти – ст. 12 ЗДПЛ, ст. 17 МПГПП, ст. 8 ЄКПЛ – задали універсальні рамки для гарантування та забезпечення захисту приватності особи [1–3]. Європейський суд з прав людини наповнив їх змістом, конкретизувавши вимоги якості закону, незалежного контролю, чітких підстав, строків та процедур зберігання/знищення даних, а також критерії «достатніх і релевантних підстав» у сфері таємного нагляду й перехоплень [15–19; 22–23; 24–28]. На рівні права ЄС, у відповідь на розвиток цифрових технологій Суд ЄС відкинув моделі загального й недиференційованого зберігання трафіку/локалізації та поставив умову «сутнісної рівноцінності» захисту при трансграничних передачах даних [10–14]. Отож приватність, так би мовити, перетворилася на правовий режим: із матеріальними (об'єкт, обсяг, межі) та процесуальними (контроль, підзвітність, засоби захисту) гарантіями.

Цифрова доба: дані, нагляд і європейська модель. У цифровому середовищі фокус уваги поступово перейшов із простору до даних, а право ЄС відповіло на це двома рівнями правового регулювання: конституційними гарантіями приватного життя/даних (ст. 7–8 Хартії ЄС) та детальними регуляторними вимогами GDPR/ePrivacy щодо мети обробки, мінімізації, підзвітності та безпеки [8, ст. 5 (1)(b),(c); 9, преамбула].

Надалі межі втручання окреслив Суд ЄС низкою прецедентів. У справі *Digital Rights Ireland* він визнав недійсною Директиву про зберігання даних, бо та запроваджувала загальне та недиференційоване зберігання трафіку/локалізації без чітких меж мети, строків і доступу, а також без достатніх запобіжників проти зловживань (порушення принципу пропорційності) [10, § § 56–69]. У *Tele2/Watson* Суд уточнив цей стандарт: загальне недиференційоване зберігання було визнано несумісним з правом ЄС, а натомість допустимим визнається лише цільове, пов'язане з боротьбою зі злочинністю, за попереднім контролем суду чи незалежного органу та з реальними процесуальними гарантіями доступу [11, § § 99–112].

Спори про трансфер даних за межі ЄС задали «еталон рівноцінності». У *Schrems I* Суд скасував механізм *Safe Harbor*, наголосивши, що треті держави повинні забезпечувати рівноцінну по суті охорону, включно з ефективними засобами правового захисту від державного доступу [12, § § 94–106]. У *Schrems II* Суд підтвердив дійсність стандартних договірних положень, але визнав недійсним *Privacy Shield*, оскільки державний нагляд у США і відсутність повноцінного судового захисту не забезпечували «сутісно рівноцінного» рівня гарантій; отже, експортер даних має оцінювати правовий режим країни-одержувача й застосовувати додаткові заходи, якщо потрібно [13, § § 126–147; 184–202].

Нарешті, у *La Quadrature du Net* Суд підтвердив заборону загального зберігання й дозволив лише виняткові, часово обмежені режими з міркувань національної безпеки за умови суворого незалежного контролю; для IP-адрес – можливим стало лише цільове зберігання з жорсткими фільтрами доступу [14, § § 133–139; 168–172].

Підхід ЄСПЛ до стратегічних перехоплень тут концептуально співзвучний. У справах *Big Brother Watch* та *Centrum för Rättvisa* Суд не відкинув «масове» перехоплення як таке, але поставив високі процесуальні вимоги: «якість закону» (доступність, передбачуваність, достатня визначеність), чіткі категорії цілей і типів даних, попередній незалежний дозвіл, багаторівневий нагляд, строки зберігання/знищення, внутрішні фільтри (селектори), а також – за можливості – повідомлення особи *ex post* [22, § § 325–363; 23, § § 260–276].

Разом окреслені нововведення сформували європейський конституційно-правовий каркас даних, що ґрунтується на таких засадах, як недопустимість загального й недиференційованого зберігання; обов'язковість цільовості, строків, незалежного попереднього контролю й реальних процесуальних запобіжників; а для трансферів – вимога сутісно рівноцінних гарантій у державі-одержувачі [11, § § 99–112; 13, § § 184–202].

Конституційно-правовий режим приватності: поняття та принципи. Під «конституційно-правовим режимом приватності» далі розуміємо сукупність принципів, норм, правил та процедур, що визначають обсяг приватної сфери особи, умови та межі допустимого втручання, а також встановлюють інституційні механізми контролю, захисту та її забезпечення.

Принципи цього режиму охоплюють три основні групи засад, кожна з яких відображає специфічні аспекти правового регулювання приватної сфери. Перша група включає матеріально-правові принципи, що визначають змістовні межі

допустимого втручання. Центральне місце серед них займає принцип законності і «якості закону», який вимагає не лише формальної наявності правової підстави для втручання, а і її змістовної відповідності стандартам доступності (публічність та зрозумілість норм для громадян), передбачуваності (можливість особи передбачити правові наслідки своїх дій) та достатньої визначеності (точність формулювання норм, що виключає свавілля правозастосувачів). Другим фундаментальним принципом цієї групи є принцип легітимної мети, який встановлює обмежений, вичерпний перелік цілей, що можуть виправдовувати втручання у приватну сферу – національна безпека, громадський порядок, запобігання злочинності, захист прав інших осіб, що унеможлиблює довільне розширення підстав для обмеження приватності.

Друга група охоплює процедурно-правові засади, які регламентують порядок та умови здійснення втручання у приватну сферу. Основним є принцип необхідності в демократичному суспільстві, що передбачає триступеневу перевірку: придатності обраних правових засобів для досягнення заявленої мети (інструмент повинен бути об'єктивно здатним вирішити проблему), нагальності потреби у втручанні (існування реальної та актуальної загрози, що вимагає негайного реагування) та наявності менш обтяжливих альтернатив (обов'язок обрати найм'якший із можливих способів досягнення мети). Принцип пропорційності *stricto sensu* забезпечує справедливе співвідношення між тяжкістю втручання у приватне життя особи та важливістю соціального інтересу, що підлягає захисту, вимагаючи проведення конкретного балансування у кожній окремій ситуації. Принцип незалежного нагляду встановлює обов'язковість попереднього або наступного контролю з боку судових органів чи незалежних адміністративних інституцій, що володіють достатніми повноваженнями для ефективної перевірки законності та обґрунтованості втручання.

Третю групу складають інституційно-правові принципи, що визначають розподіл відповідальності та механізми забезпечення захисту приватності. Принцип підзвітності володільця даних (англ. *accountability*) переносить тягар доведення правомірності обробки персональних даних на суб'єкта, який здійснює таку обробку, вимагаючи від нього не лише дотримання встановлених правил, а й документального підтвердження такого дотримання через ведення реєстрів обробки, проведення оцінки впливу на захист даних, упровадження технічних та організаційних заходів безпеки. Принцип ефективних засобів правового захисту гарантує особі реальну можливість оскаржити порушення її права на приватність через доступні, швидкі та результативні процедури, включаючи судовий захист, адміністративні скарги, відшкодування шкоди та припинення протиправних дій.

Конституційно-правове регулювання приватності в Україні зазнає фундаментального впливу через практику ЄСПЛ, оскільки згідно зі ст. 17 Закону України «Про виконання рішень та застосування практики Європейського суду з прав людини» суди України зобов'язані застосовувати практику ЄСПЛ як джерело права при розгляді справ. Цей вплив проявляється у систематичному запозиченні та адаптації європейських стандартів захисту приватності українською правовою системою. Зокрема, принцип «якості закону» отримав свою класичну інтерпретацію у справі *Sunday Times v. United Kingdom* (§ 49), де ЄСПЛ встановив, що правова норма має бути не лише офіційно оприлюдненою, а й сформульованою доволі точно, щоб особа могла «передбачити, принаймні за допомогою відповідних консультацій, якщо це необхідно, наслідки, які може спричинити певна дія». Трикомпонентний тест на пропорційність набув своєї остаточної формули у справі *Handyside v. United Kingdom* (§ 48-49), де Суд систематизував вимоги до законності підстави втручання, легітимності переслідуваної мети та її необхідності в демократичному суспільстві,

підкресливши, що остання вимога означає існування «нагальної соціальної потреби» в обмеженні права.

Особливо детально принципи захисту приватності у сфері масового спостереження були розроблені в новітній практиці ЄСПЛ. У справі *Big Brother Watch and Others v. United Kingdom* (§ § 325-363) Суд встановив вісім «мінімальних гарантій», які повинен містити національний закон про стратегічні перехоплення: визначення категорій осіб, що підлягають нагляду; характер правопорушень, що можуть служити підставою; обмеження тривалості нагляду; процедуру дослідження, використання та зберігання отриманої інформації; запобіжні заходи при передачі даних третім особам; обставини знищення записів; процедури нагляду за дотриманням цих вимог. У справі *Centrum för Rättvisa v. Sweden* (§ § 260-276) ці вимоги було уточнено щодо необхідності попереднього судового дозволу або контролю з боку незалежного органу, що володіє достатніми повноваженнями для ефективного нагляду за розвідувальною діяльністю. В європейській практиці ці принципи закріплені у ст. 8 ЄКПЛ і розгорнуті в низці рішень ЄСПЛ [15–19], а в праві ЄС – деталізовані через регуляторні акти (*GDPR*, *ePrivacy*) і прецеденти Суду ЄС [8–14], створюючи комплексну систему багаторівневого захисту приватної сфери особи.

Українська модель у цьому відношенні спирається на ст. 30–32 Конституції України (недоторканність житла; таємниця листування й інших комунікацій; заборона збирання, зберігання, використання і поширення конфіденційної інформації без згоди, за винятками, визначеними законом) [42]. Процесуальний каркас забезпечує насамперед КПК (судовий контроль за негласними слідчими (розшуковими) діями, закритий перелік заходів, строки, підстави; доктрина недопустимості доказів при порушенні процедури) та ЦПК (розкриття банківської таємниці) [48–49; 54]. Зі свого боку, спеціальні закони визначають рамки ОРД та контррозвідувальних заходів, а також режими електронних комунікацій і персональних даних [43–47]. КСУ, зокрема в рішеннях № 12-рп/2011, № 2-рп/2012, № 7-р/2018, конкретизував конституційне розуміння «якісного закону», вимоги пропорційності, межі доступу до інформації про особу та стандарт судового контролю [50–52; 53]. Отож національний порядок у принципах збігається з європейськими підходами; питання – у фактичній імплементації запобіжників (судовий дозвіл, журналювання доступів, строки зберігання/знищення, інформування *ex post*, інституційний нагляд).

Континентальна та англо-американська перспективи: витоки, акценти, наслідки для сучасного правового регулювання приватності. Порівняння двох провідних правових сімей – континентальної (романо-германської) та англо-американської (*common law*) – демонструє не лише різні історичні стартові майданчики, а й відмінні способи оцінювання, які, зрештою, формують різні конфігурації конституційно-правового режиму приватності. Можна узагальнити ці міркування у такий спосіб: континентальна традиція виходить з антропоцентричної конституційної гідності та особистісних прав (нім. *Allgemeines Persönlichkeitsrecht* – загальне право особистості), тоді як загальне право історично спиралася на свободу, власність і процесуальні стримування влади (заборона «загальних ордерів», судовий контроль), трансформуючи приватність спершу в деліктну, а потім – у конституційну категорію.

Останнє положення варто пояснити детальніше. По-перше, в континентальній Європі приватність рано «прив'язується» до гідності та автономії особи як до концептуального ядра. Символічною в цьому стосунку є постанова Федерального конституційного суду Німеччини у справі про перепис населення (нім. *Volkszählungsurteil*,

1983), яка сформулювала право на інформаційне самовизначення (право контролювати розкриття та використання відомостей про себе) як похідне від людської гідності та загального права на вільний розвиток особистості [41].

У Європейському Союзі це мислення інституціоналізоване «подвійною вертикаллю» Хартії ЄС: ст. 7 (право на повагу до приватного і сімейного життя) та ст. 8 (окреме право на захист персональних даних), що отримало регуляторне втілення у GDPR та суміжних актах (англ. *accountability* – підзвітність володільця даних; *privacy by design/by default* – захист за задумом/за замовчуванням) [4; 8; 9].

По-друге, в загальному праві приватність «народжується» з процесуальних (процедурних) бар'єрів проти вторгнення у житло й кореспонденцію, а також із захисту конфіденційної інформації. Ранні англійські прецеденти – *Semayne's Case* (обов'язок попередження при проникненні до житла), *Entick v. Carrington* (заборона «general warrants»), *Prince Albert v. Strange* (превентивний захист конфіденційних зображень через судову заборону – англ. *injunction*) – виробили своєрідну «юридичну граматику» приватної сфери [30–32]. Американська традиція, своєю чергою, проходить шлях від «поштової та паперової таємниці» (*Ex parte Jackson*; *Boyd*) до деліктної теорії Воррена-Брандейса і, згодом, до конституційної доктрини «обґрунтованого очікування приватності» (англ. *reasonable expectation of privacy*) у *Katz v. United States* [33–36; 55, 56]. У цифрову добу Верховний суд США уточнює межі доступу до смартфонів і геолокаційних метаданих (*Riley v. California*; *Carpenter v. United States*), водночас зберігаючи дискусійну «доктрину третьої сторони» (англ. *third-party doctrine* – зменшення очікування приватності щодо даних, добровільно переданих провайдером) поза межами вузько окреслених винятків [39–40; 38].

По-третє, наслідки цих витоків – різні процесуальні профілі сучасного контролю. У Європі Суд ЄС відкидає загальне й недиференційоване зберігання трафіку/локалізації та вимагає «сутісно рівноцінного» (англ. *essentially equivalent*) захисту при трансферах даних за межі ЄС (*Digital Rights Ireland*; *Tele2/Watson*; *Schrems I/II*; *La Quadrature du Net*) [10–14]. ЄСПЛ, у резонансних справах про стратегічне перехоплення (*Big Brother Watch*; *Centrum för Rättvisa*), також наполягає на «якості закону», попередньому незалежному контролю, обмежених строках, фільтрах і механізмах повідомлення *ex post*, коли це не руйнує мету заходу [22, 23].

У США ж стандарти формуються через комбінацію прецедентних рішень у межах Четвертої поправки і секторальних законів; конституційні критерії фокусуються на тому, чи порушує захід «обґрунтоване очікування приватності» в конкретних категоріях даних (уміст. пристрою, CSLI, поштові відправлення), тоді як універсального «права на дані» у вигляді, подібному до ст. 8 Хартії ЄС, не існує [35].

Нарешті, в прикладному вимірі (і це особливо важливо для законодавця та судів) континентальна модель більше тяжіє до екс-анте гарантій і системної підзвітності володільців даних, тоді як загальне право – до екс-пост контролю судом конкретних втручань з акцентом на доказуванні «необґрунтованості» пошуку/вилучення. Утім, міждержавний діалог та притаманна останньому конвергенція поступово зближують підходи правового регулювання приватності: європейська практика посилює інструменти ефективного засобу правового захисту, а американська, зі свого боку, – чутливість до цифрових контекстів (смартфони, довготрекінгові метадані), що де-факто обмежує класичну *third-party doctrine* [22–23; 39–40; 10–14].

Отже, витoki приватності в обох сім'ях різні, проте сучасний конституційно-правовий режим у Європі та США збігається у визначальному відношенні: *приватність не може бути «функцією зручності» влади чи бізнесу; втручання повинно мати чітку, зрозумілу й передбачувану у своєму застосуванні правову основу* (англ. *quality of law* – якість закону), *легітимну мету, доведену необхідність*

і пропорційність, підлягати незалежному контролю і відкривати ефективні засоби правового захисту [3–4; 8–9; 15–19; 22–23; 10–14; 35–40; 41]. У подальшому ці принципи проєктуються на український конституційний лад з урахуванням специфіки ст. 30–32 Конституції України та практики Конституційного Суду України [42; 50–52].

Висновки. Історична еволюція приватності від римських інститутів *dominium* та *domus* через середньовічні корпоративні таємниці до сучасного конституційно-правового регулювання демонструє послідовну трансформацію від територіально-станових привілеїв до універсальних прав людини. Ключові віхи цього процесу – від *Magna Carta* та *Semayne's Case* до класичної статті *Warren-Brandeis* (1890) та практики ЄСПЛ у справах *Big Brother Watch* і *Schrems* – засвідчують, що кожна епоха формувала власні відповіді на технологічні та політичні загрози для приватності, створюючи «правовий інвентар» для наступних поколінь.

Принципи сучасного конституційно-правового режиму приватності структуруються у три групи засад. Матеріально-правові принципи (законність і «якість закону», легітимна мета) визначають змістовні межі втручання та вимагають доступності, передбачуваності та достатньої визначеності правових норм. Процедурно-правові принципи (необхідність у демократичному суспільстві, пропорційність, незалежний нагляд) регламентують порядок здійснення втручання через триступеневу перевірку придатності, нагальності та менш обтяжливих альтернатив. Інституційно-правові принципи (підзвітність, ефективні засоби захисту) забезпечують розподіл відповідальності та реальні механізми відновлення порушених прав.

Конституційно-правове регулювання приватності в Україні формується під визначальним впливом практики ЄСПЛ. Європейські стандарти, розроблені у справах *Sunday Times* (принцип «якості закону»), *Handyside* (тест пропорційності), *Big Brother Watch* (мінімальні гарантії при масовому спостереженні), інтегруються в українську правозастосовну практику та створюють єдиний простір захисту приватної сфери. Право ЄС через прецеденти *Digital Rights Ireland*, *Schrems I* і *II*, *La Quadrature du Net* встановлює заборону загального недиференційованого зберігання даних та вимагає «сутнісно рівноцінного» захисту при трансграничних передачах.

Для українського правопорядку викладене диктує необхідність системної імплементації європейських стандартів у всіх сферах регулювання приватності.

Список використаних джерел

1. Загальна декларація прав людини : міжнародний документ від 10.12.1948 р.
2. Міжнародний пакт про громадянські і політичні права : міжнародний договір від 16.12.1966 р. (ст. 17).
3. Європейська конвенція про захист прав людини і основоположних свобод : міжнародний договір від 04.11.1950 р. (ст. 8).
4. Хартія основоположних прав Європейського Союзу : міжнародний документ від 07.12.2000 р. (офіц. опубл. – 2012/С 326/02) (ст. 7–8).
5. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» : міжнародний договір від 28.01.1981 р.
6. Протокол CETS 223 (Convention 108+) до Конвенції № 108 : міжнародний документ від 10.10.2018 р.
7. OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data : міжнародні керівні принципи, 1980 (ред. 2013).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) : регламент ЄС від 27.04.2016 р.

9. Directive 2002/58/EC of the European Parliament and of the Council (ePrivacy) : директива ЄС від 12.07.2002 р.
10. Joined Cases C-293/12 і C-594/12, Digital Rights Ireland : рішення Суду ЄС від 08.04.2014 р.
11. Joined Cases C-203/15 і C-698/15, Tele2 Sverige AB / Watson : рішення Суду ЄС від 21.12.2016 р.
12. Case C-362/14, Schrems : рішення Суду ЄС від 06.10.2015 р.
13. Case C-311/18, Schrems II : рішення Суду ЄС від 16.07.2020 р.
14. Joined Cases C-511/18, C-512/18, C-520/18, La Quadrature du Net and Others : рішення Суду ЄС від 06.10.2020 р.
15. Klass and Others v. Germany : рішення ЄСПЛ від 06.09.1978 р., заява № 5029/71.
16. Malone v. the United Kingdom : рішення ЄСПЛ від 02.08.1984 р., заява № 8691/79.
17. Leander v. Sweden : рішення ЄСПЛ від 26.03.1987 р., заява № 9248/81.
18. Niemietz v. Germany : рішення ЄСПЛ від 16.12.1992 р., заява № 13710/88.
19. Handyside v. the United Kingdom : рішення ЄСПЛ від 07.12.1976 р., заява № 5493/72.
20. Roman Zakharov v. Russia [GC] : рішення ЄСПЛ від 04.12.2015 р., заява № 47143/06.
21. Szabó and Vissy v. Hungary : рішення ЄСПЛ від 12.01.2016 р., заява № 37138/14.
22. Big Brother Watch and Others v. the United Kingdom [GC] : рішення ЄСПЛ від 25.05.2021 р., заяви № 58170/13, 62322/14, 24960/15.
23. Centrum för Rättvisa v. Sweden [GC] : рішення ЄСПЛ від 25.05.2021 р., заява № 35252/08.
24. Bărbulescu v. Romania [GC] : рішення ЄСПЛ від 05.09.2017 р., заява № 61496/08.
25. López Ribalda and Others v. Spain [GC] : рішення ЄСПЛ від 17.10.2019 р., заяви № 1874/13, 8567/13.
26. Axel Springer AG v. Germany [GC] : рішення ЄСПЛ від 07.02.2012 р., заява № 39954/08.
27. Von Hannover v. Germany (No. 2) [GC] : рішення ЄСПЛ від 07.02.2012 р., заяви № 40660/08, 60641/08.
28. Antović and Mirković v. Montenegro : рішення ЄСПЛ від 28.11.2017 р., заява № 70838/13.
29. Magna Carta (1215) : конституційний акт середньовічної Англії, 1215 р.
30. Semayne's Case (1604) : рішення Court of King's Bench // Coke's Reports, vol. 5, 91a.
31. Entick v. Carrington (1765) : рішення King's Bench // 19 Howell's State Trials 1029.
32. Prince Albert v. Strange (1849) : рішення High Court of Chancery // 2 De Gex & Smale 652; 64 ER 293.
33. Ex parte Jackson, 96 U.S. 727 (1878) : рішення Верховного суду США, 1878 р.
34. Boyd v. United States, 116 U.S. 616 (1886) : рішення Верховного суду США, 1886 р.
35. Griswold v. Connecticut, 381 U.S. 479 (1965) : рішення Верховного суду США, 1965 р.
36. Katz v. United States, 389 U.S. 347 (1967) : рішення Верховного суду США, 1967 р.
37. Whalen v. Roe, 429 U.S. 589 (1977) : рішення Верховного суду США, 1977 р.
38. Smith v. Maryland, 442 U.S. 735 (1979) : рішення Верховного суду США, 1979 р.
39. Riley v. California, 573 U.S. 373 (2014) : рішення Верховного суду США, 2014 р.
40. Carpenter v. United States, 138 S. Ct. 2206 (2018) : рішення Верховного суду США, 2018 р.
41. Bundesverfassungsgericht. Volkszählungsurteil : рішення Федерального конституційного суду Німеччини від 15.12.1983 р., BVerfGE 65, 1 (право на інформаційне самовизначення).
42. Конституція України : Закон України від 28.06.1996 р. (ст. 30–32).
43. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI.
44. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX.
45. Про інформацію : Закон України від 02.10.1992 р. (зі змін.).
46. Про оперативно-розшукову діяльність : Закон України від 18.02.1992 р.
47. Про контророзвідувальну діяльність : Закон України від 26.12.2002 р. № 374-IV.
48. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. (розділи про НСРД).

49. Спільний наказ № 114/1042/516/1199/936/1687/5 від 16.11.2012 р. «Інструкція з організації негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні».
50. Рішення Конституційного Суду України № 12-рп/2011 від 20.10.2011 р. (щодо недоторканності житла).
51. Рішення Конституційного Суду України № 2-рп/2012 від 20.01.2012 р. (офіц. тлумачення ст. 32, 34 Конституції України).
52. Рішення Конституційного Суду України № 7-р/2018 від 11.10.2018 р. (персональні дані; баланс ст. 32 Конституції та ст. 8 ЄКПЛ).
53. Рішення Конституційного Суду України від 05.03.2003 р. (банківська таємниця; межі доступу органів держави).
54. Верховний Суд (Касаційний кримінальний суд) : Постанова від 17.01.2019 р. у справі № 740/1244/16-к (НСПД; допустимість доказів).
55. Warren S. D., Brandeis L. D. The Right to Privacy. *Harvard Law Review*. 1890. Vol. 4. No. 5. P. 193–220.
56. Prosser W. L. Privacy. *California Law Review*. 1960. Vol. 48. No. 3. P. 383–423.
57. Westin A. F. Privacy and Freedom. New York : Atheneum, 1967. 487 p.
58. Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life : монографія. Stanford : Stanford University Press, 2010. 304 p.
59. Alexy R. A Theory of Constitutional Rights : монографія. Oxford : Oxford University Press, 2002. 462 p.
60. Barak A. Proportionality: Constitutional Rights and Their Limitations : монографія. Cambridge : Cambridge University Press, 2012. 488 p.
61. Kumm M. Constitutional Rights as Principles. *International Journal of Constitutional Law*. 2004. Vol. 2. No. 3. P. 574–596.
62. Kuner C., Bygrave L., Docksey C. (eds.). The EU General Data Protection Regulation (GDPR): A Commentary : монографія. Oxford : Oxford University Press, 2020. 1520 p.
63. FRA (EU Agency for Fundamental Rights). Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU : звіт. Vienna : FRA, 2017 (оновл. 2021).
64. European Data Protection Board. Guidelines on Data Protection Impact Assessment (DPIA) : керівництво. Brussels : EDPB, 2017 (оновл.).
65. Погорілко В. Ф. (ред.) Конституційне право України : підручник. Київ : Наукова думка, 2006. 728 с.
66. Федоренко В. Л. Конституційне право України : підручник. Київ : Ліра-К, 2016. 824 с.
67. Барабаш Ю. Г. Конституційне право України : навч. посіб. Харків : Право, 2008. 416 с.
68. Бориславська О. М., Барабаш Ю. Г., Козюбра М. І. та ін. Конституційне право : підручник. Київ : НАУКМА / ОБСЄ, 2021. 640 с.
69. Різник С. В. Про поняття конституційності нормативних актів. *Український часопис конституційного права*. 2020. № 2. С. 26–37.
70. Різник С. В. Застосування судами Конституції України : монографія (колект. авт.). Київ : Верховний Суд, 2022. 380 с.
71. Lewis C. T., Short C. A Latin Dictionary. Oxford : Clarendon Press, 1879. Perseus Project. Стаття «privatus». URL: <https://anastrophe.uchicago.edu/perseus/LewisShort.html> (дата звернення: 02.11.2025).
72. Liddell H. G., Scott R., Jones H. S., McKenzie R. A Greek–English Lexicon. 9-th ed. Oxford : Clarendon Press, 1940. Logeion (University of Chicago). Стаття «ιδιώτης». URL: <https://logeion.uchicago.edu/ιδιώτης> (дата звернення: 02.11.2025).
73. Harper D. Online Etymology Dictionary. Стаття «privacy». URL: <https://www.etymonline.com/word/privacy> (дата звернення: 02.11.2025).

74. Centre National de Ressources Textuelles et Lexicales (CNRTL). *Trésor de la langue française informatisé* (TLFi). Стаття «privé, -ée». URL: <https://www.cnrtl.fr/definition/priv%C3%A9>- (дата звернення: 02.11.2025).
75. Code civil. Article 9. Legifrance. URL: https://www.legifrance.gouv.fr/codes/article_lc/-LEGIARTI000006419288 (дата звернення: 02.11.2025).

References

1. Zahalna deklaratsiia prav liudyny : mizhnarodnyi dokument (10.12.1948 r.).
2. Mizhnarodnyi pakt pro hromadianski i politychni prava : mizhnarodnyi dohovir (16.12.1966 r.) (st. 17).
3. Ievropeiska konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod : mizhnarodnyi dohovir (04.11.1950 r.) (st. 8).
4. Khartiia osnovopolozhnykh prav Ievropeiskoho Soiuzu : mizhnarodnyi dokument (07.12.2000 r.) (ofits. opubl. – 2012/C 326/02) (st. 7–8).
5. Konventsiia Rady Yevropy № 108 «Pro zakhyst osib u zv'iazku z avtomatyzovanoi obrobkoiu personalnykh danykh»: mizhnarodnyi dohovir (28.01.1981 r.).
6. Protokol CETS 223 (Convention 108+) do Konventsii No. 108 : mizhnarodnyi dokument (10.10.2018 r.).
7. OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data : mizhnarodni kerivni pryntsypy, 1980 (red. 2013).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) : rehlament YeS (27.04.2016 r.).
9. Directive 2002/58/EC of the European Parliament and of the Council (ePrivacy) : dyrektyva YeS (12.07.2002 r.).
10. Joined Cases C-293/12 i C-594/12. Digital Rights Ireland : rishennia Sudu YeS (08.04.2014 r.).
11. Joined Cases C-203/15 i C-698/15, Tele2 Sverige AB / Watson : rishennia Sudu YeS (21.12.2016 r.).
12. Case C-362/14, Schrems : rishennia Sudu YeS (06.10.2015 r.).
13. Case C-311/18, Schrems II : rishennia Sudu YeS (16.07.2020 r.).
14. Joined Cases C-511/18, C-512/18, C-520/18. La Quadrature du Net and Others : rishennia Sudu YeS (06.10.2020 r.).
15. Klass and Others v. Germany : rishennia YeSP (06.09.1978 r.), zaiava No. 5029/71.
16. Malone v. the United Kingdom : rishennia YeSP (02.08.1984 r.), zaiava No. 8691/79.
17. Leander v. Sweden : rishennia YeSP (26.03.1987 r.), zaiava No. 9248/81.
18. Niemietz v. Germany : rishennia YeSP (16.12.1992 r.), zaiava No. 13710/88.
19. Handyside v. the United Kingdom : rishennia YeSP (07.12.1976 r.), zaiava No. 5493/72.
20. Roman Zakharov v. Russia [GC] : rishennia YeSP (04.12.2015 r.), zaiava No. 47143/06.
21. Szabó and Vissy v. Hungary : rishennia YeSP (12.01.2016 r.), zaiava No. 37138/14.
22. Big Brother Watch and Others v. the United Kingdom [GC] : rishennia YeSP (25.05.2021 r.), zaiavy No. 58170/13, 62322/14, 24960/15.
23. Centrum för Rättvisa v. Sweden [GC] : rishennia YeSP (25.05.2021 r.), zaiava No. 35252/08.
24. Bărbulescu v. Romania [GC] : rishennia YeSP (05.09.2017 r.), zaiava No. 61496/08.
25. López Ribalda and Others v. Spain [GC] : rishennia YeSP (17.10.2019 r.), zaiavy No. 1874/13, 8567/13.
26. Axel Springer AG v. Germany [GC] : rishennia YeSP (07.02.2012 r.), zaiava No. 39954/08.
27. Von Hannover v. Germany (No. 2) [GC] : rishennia YeSP (07.02.2012 r.), zaiavy No. 40660/08, 60641/08.
28. Antović and Mirković v. Montenegro : rishennia YeSP (28.11.2017 r.), zaiava No. 70838/13.
29. Magna Carta (1215) : konstytutsiinyi akt seredniovichnoi Anhlii, 1215 r.

30. *Semayne's Case* (1604) : rishennia Court of King's Bench. *Coke's Reports*, 5, 91a.
31. *Entick v. Carrington* (1765) : rishennia King's Bench. 19 *Howell's State Trials*, 1029.
32. *Prince Albert v. Strange* (1849) : rishennia High Court of Chancery. 2 *De Gex & Smale* 652; 64 ER 293.
33. *Ex parte Jackson*, 96 U.S. 727 (1878) : rishennia Verkhovnoho sudu SSHA.
34. *Boyd v. United States*, 116 U.S. 616 (1886) : rishennia Verkhovnoho sudu SSHA.
35. *Griswold v. Connecticut*, 381 U.S. 479 (1965) : rishennia Verkhovnoho sudu SSHA.
36. *Katz v. United States*, 389 U.S. 347 (1967) : rishennia Verkhovnoho sudu SSHA.
37. *Whalen v. Roe*, 429 U.S. 589 (1977) : rishennia Verkhovnoho sudu SSHA.
38. *Smith v. Maryland*, 442 U.S. 735 (1979) : rishennia Verkhovnoho sudu SSHA.
39. *Riley v. California*, 573 U.S. 373 (2014) : rishennia Verkhovnoho sudu SSHA.
40. *Carpenter v. United States*, 138 S. Ct. 2206 (2018) : rishennia Verkhovnoho sudu SSHA.
41. Bundesverfassungsgericht. Volkszählungsurteil: rishennia Federalnoho konstytutsiinoho sudu Nimechchyny (15.12.1983 r.), BVerfGE 65, 1 (pravo na informatsiine samovyznachennia).
42. Konstytutsiia Ukrainy : Zakon Ukrainy (28.06.1996 r.) (st. 30–32).
43. Pro zakhyst personalnykh danykh : Zakon Ukrainy (01.06.2010 r.) No. 2297-VI.
44. Pro elektronni komunikatsii : Zakon Ukrainy (16.12.2020 r.) No. 1089-IX.
45. Pro informatsiiu : Zakon Ukrainy (02.10.1992 r.) (zi zmin.).
46. Pro operatyvno-rozhukovu diialnist : Zakon Ukrainy (18.02.1992 r.).
47. Pro kontrozviduvalnu diialnist : Zakon Ukrainy (26.12.2002 r.).
48. Kryminalnyi protsesualnyi kodeks Ukrainy : Zakon Ukrainy (13.04.2012 r.) (rozdily pro NSRD).
49. Spilnyi nakaz (16.11.2012 r.). No. 114/1042/516/1199/936/1687/5. Instrukttsiia z orhanizatsii nehlasnykh slidchykh (rozshukovykh) dii ta vykorystannia yikh rezultativ u kryminalnomu provadzhenni.
50. Rishennia Konstytutsiinoho Sudu Ukrainy (20.10.2011 r.). No. 12-rp/2011 (shchodo nedotorkannosti zhytla).
51. Rishennia Konstytutsiinoho Sudu Ukrainy (20.01.2012 r.). No.2-rp/2012 (ofits. tlumachennia st. 32, 34 Konstytutsii Ukrainy).
52. Rishennia Konstytutsiinoho Sudu Ukrainy (11.10.2018 r.). No. 7-r/2018 (personalni dani; balans st. 32 Konstytutsii ta st. 8 YeKPL).
53. Rishennia Konstytutsiinoho Sudu Ukrainy (05.03.2003 r.) (bankivska taiemnytsia; mezhi dostupu orhaniv derzhavy).
54. Verkhovnyi Sud (Kasatsiinyi kryminalnyi sud) : Postanova (17.01.2019 r. u spravi No. 740/1244/16-k) (NSRD; dopustymist dokaziv).
55. Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4, 5, 193–220.
56. Prosser, W. L. (1960). Privacy. *California Law Review*, 48, 3, 383–423.
57. Westin, A. F. (1967). *Privacy and Freedom*. New York : Atheneum.
58. Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford : Stanford University Press.
59. Alexy, R. (2002). *A Theory of Constitutional Rights*. Oxford : Oxford University Press.
60. Barak, A. (2012). *Proportionality: Constitutional Rights and Their Limitations*. Cambridge : Cambridge University Press.
61. Kumm, M. (2004). Constitutional Rights as Principles. *International Journal of Constitutional Law*, 2, 3, 574–596.
62. Kuner, C., Bygrave, L., & Docksey, C. (eds.). (2020). *The EU General Data Protection Regulation (GDPR) : A Commentary*. Oxford : Oxford University Press.
63. FRA (EU Agency for Fundamental Rights). *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU*. Vienna : FRA, 2017 (updated 2021).

64. European Data Protection Board. Guidelines on Data Protection Impact Assessment (DPIA). Brussels : EDPB, 2017 (updated).
65. Pohorilko, V. F. (eds.). (2006). *Konstytutsiine pravo Ukrainy* : pidruchnyk. Kyiv : Naukova dumka.
66. Fedorenko, V. L. (2016). *Konstytutsiine pravo Ukrainy* : pidruchnyk. Kyiv : Lira-K.
67. Barabash, Yu. H. (2008). *Konstytutsiine pravo Ukrainy* : navchalnyi posibnyk. Kharkiv : Pravo.
68. Borislavska, O. M., Barabash, Yu. H., Koziubra, M. I. and others. (2021).. *Konstytutsiine pravo* : pidruchnyk. Kyiv : NaUKMA / OBSYe.
69. Riznyk, S. V. (2020). Pro poniattia konstytutsiinosti normatyvnykh aktiv. *Ukrainskyi chasopys konstytutsiinoho prava*, 2, 26–37.
70. Riznyk, S. V. (2022). *Zastosuvannia sudamy Konstytutsii Ukrainy* : monohrafiia (kolekt. avt.). Kyiv : Verkhovnyi Sud.
71. Lewis, C. T., & Short, C. (1879). A Latin Dictionary. Oxford : Clarendon Press. *Perseus Project. Statia «privatus», 2 (2025)*. Retrieved from <https://anastrophe.uchicago.edu/perseus/-LewisShort.html>.
72. Liddell, H. G., Scott, R., Jones, H. S., & McKenzie, R. (1940). *A Greek-English Lexicon*. 9-th ed. Oxford : Clarendon Press. Logeion (University of Chicago). Statia «idiotes». (Nov. 2 2025). Retrieved from <https://logeion.uchicago.edu/>.
73. Harper, D. (2025). *Online Etymology Dictionary*. Statia «privacy». Nov. 2. Retrieved from <https://www.etymonline.com/word/privacy>.
74. Centre National de Ressources Textuelles et Lexicales (CNRTL). Trsor de la langue franaise informati© (TLFi). Statia «prive, -ee». (Nov 2, 2025). Retrieved from <https://www.cnrtl.fr/-definition/priv%C3%A9>.
75. Code civil. Article 9. Legifrance. (Nov 2, 2025) Retrieved from https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419288.

GENESIS OF THE LEGAL PROTECTION OF PRIVACY

Vitalii Chornenkyi

*Ivan Franko National University of Lviv,
1, Universytetska Str., Lviv, Ukraine, 79000
e-mail: vitaliy.chornenkyi@lnu.edu.ua
ORCID ID: 0000-0001-5067-0844*

The article provides a comprehensive historical and comparative analysis of how the legal concept of privacy evolved—from its earliest manifestations in Roman and medieval law to its modern constitutional and digital dimensions. The author reconstructs the genealogy of privacy as a legal category, showing how the notion of an individual's "private sphere" gradually emerged from procedural barriers and local privileges into a universal human right protected by constitutional and international mechanisms.

The study begins with a linguistic and conceptual overview, demonstrating that in classical and Indo-European traditions, "privacy" denoted separation from the public realm and control over access to one's personal domain. The author traces this boundary through the Roman *domus* and *dominium*, the medieval concept of "house peace" (*Hausfrieden*), feudal immunities, and corporate or religious secrecy—each of which represented an early form of spatial, informational, or spiritual privacy. These premodern practices, though procedural and local, laid the groundwork for the later doctrine of inviolability of home and correspondence.

A decisive transformation occurred at the turn of the modern era, when constitutional restraints on state power—exemplified by *Magna Carta* and English common law cases such as *Semayne's Case* (1604) and *Entick v. Carrington* (1765)—established procedural guarantees

against arbitrary intrusions. The nineteenth century marked the conceptual crystallization of privacy as an autonomous right: the landmark article by Warren and Brandeis (1890) defined it as “the right to be let alone,” while subsequent U.S. jurisprudence (from *Griswold v. Connecticut* to *Carpenter v. United States*) extended protection to correspondence, communications, and digital data.

The twentieth century introduced international constitutionalization: Article 12 of the UDHR, Article 17 of the ICCPR, and Article 8 of the ECHR enshrined privacy as a fundamental human right. The European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) further defined its procedural standards—lawfulness, foreseeability, proportionality, and independent oversight—through key judgments such as *Big Brother Watch*, *Tele2/Watson*, *Schrems I/II*, and *La Quadrature du Net*. These cases shaped the modern European model, which rejects indiscriminate data retention and requires “essentially equivalent” protection in cross-border transfers.

The article conceptualizes the constitutional-legal regime of privacy as a coherent system of principles encompassing:

Substantive principles—legality, quality of law, and legitimate aim;

Procedural principles—necessity in a democratic society, proportionality, and independent supervision;

Institutional principles—accountability of data controllers and effective remedies.

In the Ukrainian context, these principles are embodied in Articles 30–32 of the Constitution, the jurisprudence of the Constitutional Court, and procedural safeguards under the Criminal Procedure Code. The national legal order, under the influence of the ECHR, is converging with European standards, though challenges remain in implementing judicial authorization, data retention limits, and post-factum notification.

Ultimately, the article demonstrates that the modern law of privacy is the result of a continuous process of juridical refinement of the boundary between the public and the private, adapting to each era’s political and technological realities. The historical trajectory—from *domus* to *data*—reveals privacy as not merely a defensive right but a dynamic constitutional regime ensuring personal autonomy, dignity, and control over information in the digital age.

Keywords: personal autonomy; dignity; proportionality; oversight; personal data.

*Стаття: надійшла до редакції 12.10.2025
прийнята до друку 21.10.2025*