

УДК 347.965:342.721:004.8

DOI <https://doi.org/10.32782/2523-4269-2026-95-114-119>

Теличко Оксана Анатоліївна,

кандидат юридичних наук, доцент,

завідувач кафедри права

(Державний університет економіки і технологій, м. Кривий Ріг)

ORCID: <https://orcid.org/0000-0003-2536-7442>



Рекун Віктор Анатолійович,

кандидат юридичних наук, доцент,

доцент кафедри права

(Державний університет економіки і технологій, м. Кривий Ріг)

ORCID: <https://orcid.org/0000-0002-2636-9426>



ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ АДВОКАТСЬКОЇ ТАЄМНИЦІ ПРИ ВИКОРИСТАННІ ХМАРНИХ СЕРВІСІВ І СИСТЕМ ШТУЧНОГО ІНТЕЛЕКТУ

*Статтю присвячено правовому режиму адвокатської таємниці в контексті використання адвокатами хмарних сервісів та штучного інтелекту іноземних провайдерів. Виявлено конкуренцію обов'язку нерозголошення адвокатської таємниці й режиму захисту персональних даних під час транскордонної передачі інформації. Запропоновано вирішення шляхом застосування принципу *lex specialis derogat generali* з пріоритетом законодавства про адвокатуру. Проаналізовано практику Європейського суду з прав людини, рекомендації CCBE та ABA, сформульовано пропозиції щодо вдосконалення законодавства.*

Ключові слова: адвокатська таємниця, хмарні сервіси, штучний інтелект, захист персональних даних, транскордонна передача даних, конфіденційність, Європейський суд з прав людини.

Постановка проблеми. Професійна діяльність адвоката дедалі більше опосередковується цифровими інструментами: підготовка процесуальних документів, аналіз матеріалів справи, пошук судової практики, переклад і транскрибування все частіше здійснюються за допомогою хмарних сервісів та інструментів штучного інтелекту, зокрема генеративних мовних моделей. Такі інструменти переважно надаються іноземними провайдерами, а введені в них дані – тексти запитів, завантажені документи, матеріали листування – можуть оброблятися на серверах поза межами України й використовуватися окремими провайдерами для подальшого вдосконалення моделей відповідно до умов конкретного сервісу. Спільною ознакою таких інструментів є передача або віддалена обробка інформації, яка потенційно містить відомості, що становлять адвокатську таємницю.

Відповідно до частини першої статті 22 Закону України «Про адвокатуру та адвокатську діяльність» адвокатською таємницею є будь-яка інформація, що стала відома адвокату про клієнта, а також документи та відомості, одержані адвокатом під час здійснення

адвокатської діяльності [1]. Стаття 10 Правил адвокатської етики закріплює збереження конфіденційності такої інформації як безумовний обов'язок адвоката щодо клієнта [2]. Жодна із цих норм не передбачає винятку для випадків, коли інформація, що становить адвокатську таємницю, вводиться адвокатом до хмарного сервісу чи інструмента штучного інтелекту, розташованого за кордоном.

Водночас передача персональних даних клієнта іноземному провайдеру підпадає під дію статті 29 Закону України «Про захист персональних даних» [3], яка відсилає до переліку держав із належним захистом персональних даних, затвердженого Кабінетом Міністрів України. Слід уточнити, що чинний перелік, затверджений постановою КМУ від 16.08.2022 № 910 [4], застосовується виключно для цілей порталу «Дія»; загального переліку для інших випадків транскордонної передачі за статтею 29 станом на час підготовки статті не затверджено, що є додатковим фактором правової невизначеності. Розширений і наближений до Регламенту GDPR 2016/679 [5] режим транскордонної передачі закладено у проєкті Закону про захист

персональних даних № 8153, який на момент завершення цього дослідження перебуває на стадії підготовки до другого читання [6].

Таким чином, виникає конкуренція двох правових режимів: адвокат, який використовує іноземний хмарний або AI-сервіс, одночасно є суб'єктом режиму адвокатської таємниці (суб'єктного за природою) і режиму захисту персональних даних (об'єктного за природою). Чинне законодавство прямо не визначає, чи є провайдер такого сервісу «третьою особою» у розумінні законодавства про адвокатуру та як співвідносяться вимоги статті 29 Закону № 2297-VI з високим рівнем гарантій нерозголошення адвокатської таємниці. На думку автора, виявлена нормативна неузгодженість має вирішуватися шляхом застосування принципу *lex specialis derogat generali*. Правове регулювання адвокатської діяльності встановлює спеціальний режим охорони професійної інформації, який передбачає вищий рівень гарантій конфіденційності порівняно із загальним режимом захисту персональних даних. Тому у випадках, коли використання хмарних сервісів або систем штучного інтелекту одночасно підпадає під дію обох законів, пріоритет доцільно надавати спеціальним гарантіям, закріпленим законодавством про адвокатуру, якщо інше прямо не встановлено законом.

Передумовою виникнення окресленої проблеми є не лише розвиток цифрових технологій, а й історично сформована модель правового регулювання адвокатської таємниці, орієнтована на міжособистісний характер відносин між адвокатом і клієнтом. Сучасні цифрові сервіси об'єктивно залучають до процесу надання правничої допомоги технологічних провайдерів, роль яких чинне законодавство належним чином не враховує. За таких умов подолання нормативної неузгодженості між правовими режимами не може обмежуватися лише вдосконаленням законодавства про захист персональних даних, а потребує переосмислення механізму охорони адвокатської таємниці з урахуванням цифровізації правничої діяльності.

Аналіз останніх досліджень і публікацій. Питання адвокатської таємниці, конфіденційності адвокатської діяльності, захисту персональних даних і цифровізації правничої професії отримали певне висвітлення в українській правовій доктрині. Зокрема, В. Заборовський у низці наукових праць дослідив поняття, правову природу, зміст і гарантії адвокатської таємниці, а також у контексті реалізації права адвоката на адвокатський запит звернувся до проблематики співвідношення адвокатської таємниці, інформації з обмеженим доступом і законодавства про захист персональних даних; В. Колонська та І. Литвинова розглядали принцип конфіденційності як одну з основ адвокатської діяльності, приділивши увагу використанню електронних технологій і систем штучного інтелекту під час надання правничої допомоги; Л. Остафійчук досліджувала питання забезпечення конфіденційності адвокатської діяльності в умовах цифровізації, а саме окремі правові аспекти використання сучасних інформаційних технологій і систем штучного інтелекту адвокатами. Водночас зазначені праці присвячені окремим аспектам досліджуваної проблематики й не містять комплексного аналізу правового забезпечення адвокатської таємниці в разі використання хмарних сервісів і систем штучного інтелекту.

Окремої уваги заслуговують новітні праці зарубіжних авторів, присвячені забезпеченню професійної конфіденційності адвоката в умовах цифрової трансформації юридичної діяльності: Дж. Е. Перлін (Jonah

E. Perlin) у своїх дослідженнях обґрунтовує необхідність розглядати конфіденційність клієнтської інформації крізь призму забезпечення її інформаційної безпеки в цифровому середовищі, зокрема під час використання хмарних технологій; Е. М. Перлман (Andrew M. Perlman) аналізує етичні аспекти використання генеративного штучного інтелекту в юридичній практиці, акцентуючи увагу на необхідності дотримання адвокатами обов'язків щодо професійної компетентності, конфіденційності клієнтської інформації та належного контролю за використанням AI.

Поряд із науковими дослідженнями зазначена проблематика активно обговорюється на рівні професійної спільноти. В Україні Вища школа адвокатури НААУ у своїх навчально-методичних заходах висвітлює практичні аспекти використання систем штучного інтелекту в адвокатській діяльності, зокрема питання забезпечення конфіденційності інформації, інформування клієнта про застосування AI, здійснення людського контролю за результатами його використання та дотримання правил адвокатської етики [7]. На міжнародному рівні відповідні рекомендаційні підходи відображені в документах CCBE – Guide on the Use of Generative AI by Lawyers [8] та Technical Guide on the Use of AI Tools and Models by Lawyers [9], а також у Formal Opinion № 512 Американської асоціації юристів [10], які містять рекомендації щодо забезпечення конфіденційності клієнтської інформації, здійснення належного людського контролю (human oversight) за використанням AI, оцінки ризиків розкриття інформації та в разі потреби отримання поінформованої згоди клієнта. Зазначені документи належать до актив soft law, не є складовою правової системи України та мають рекомендаційний характер.

Аналіз наукової літератури та професійних рекомендацій свідчить, що існуючі дослідження висвітлюють окремі питання адвокатської таємниці, конфіденційності адвокатської діяльності, інформаційної безпеки, використання генеративного штучного інтелекту та захисту legal professional privilege. Водночас у сучасній українській юридичній науці відсутнє комплексне дослідження правового забезпечення адвокатської таємниці в разі використання хмарних сервісів і систем штучного інтелекту, яке б системно поєднувало положення Закону України «Про адвокатуру та адвокатську діяльність» [1], законодавства про захист персональних даних [3], вимоги GDPR [5] та сучасні європейські підходи до правового регулювання використання цифрових технологій у правничій діяльності. Недостатньо дослідженим залишається також питання правової кваліфікації використання іноземних хмарних та AI-сервісів як форми транскордонної передачі персональних даних і його впливу на забезпечення адвокатської таємниці. Наукова новизна полягає у системному обґрунтуванні правового забезпечення адвокатської таємниці в разі використання хмарних сервісів і систем штучного інтелекту шляхом інтегрованого аналізу законодавства України, права Європейського Союзу, практики Європейського суду з прав людини та сучасних європейських підходів до регулювання цифрових технологій у правничій діяльності, а також у формулюванні пропозицій щодо вдосконалення відповідного правового регулювання. Це зумовлює актуальність і визначає предмет статті.

Метою статті є визначення правової неузгодженості між обов'язком адвоката зберігати адвокатську таємницю та вимогами законодавства про захист персональних даних щодо транскордонної передачі інформації, яка

виникає у зв'язку з використанням адвокатами хмарних сервісів та інструментів штучного інтелекту іноземних провайдерів, а також формулювання науково обґрунтованих пропозицій щодо усунення виявленої прогалини правового регулювання з урахуванням практики Європейського суду з прав людини, права Європейського Союзу та рекомендацій європейських професійних об'єднань адвокатів.

Виклад основного матеріалу. Частина перша статті 22 Закону «Про адвокатуру та адвокатську діяльність» визначає коло осіб, на яких поширюється обов'язок зберігати адвокатську таємницю: адвокат, помічник адвоката, стажист адвоката, особа, яка перебуває у трудових відносинах з адвокатом [1]. Це визначення побудовано за суб'єктним принципом: режим таємниці прив'язаний не до інформації як такої, а до осіб у трудових чи договірних відносинах з адвокатом. Провайдер хмарного сервісу чи AI-системи – зазвичай іноземна юридична особа, з якою адвокат перебуває в договірних відносинах на умовах стандартного договору приєднання, – не належить до суб'єктів, на яких стаття 22 прямо покладає обов'язок збереження адвокатської таємниці [1]. Це означає, що зобов'язання такого провайдера (якщо вони взагалі існують) впливають виключно з договору про надання послуг і його власної політики конфіденційності, зміст якої адвокат зазвичай не може узгодити індивідуально. Стаття 10 Правил адвокатської етики покладає на адвоката обов'язок дотримуватися конфіденційності [2], проте не містить спеціальних положень щодо використання зовнішніх цифрових сервісів. На відміну від цього, CCBE Guide on the Use of Generative AI by Lawyers (2025) [8] та CCBE Technical Guide on the Use of AI Tools and Models by Lawyers (2026) [9] прямо рекомендують адвокатам вживати технічних і організаційних заходів для запобігання несанкціонованому доступу до інформації клієнта та забезпечувати людський контроль (human oversight) за результатами роботи AI-систем.

Технічне керівництво CCBE звертає увагу, що дані, введені користувачем, та отримана відповідь зазвичай проходять через інфраструктуру, яку він не контролює: навіть за «наскрізного шифрування» неможливо достеменно встановити, хто – включно з субпідрядниками провайдера – може отримати доступ до цих даних [9]. Частина комерційних AI-сервісів за замовчуванням використовує введені дані для донавчання моделі, якщо користувач не активував функцію відмови (opt-out) [8].

Якщо провайдер використовує введені адвокатом дані для донавчання власної моделі, він не просто обробляє їх за дорученням адвоката (як «розпорядник» за Законом «Про захист персональних даних» [3]), а самостійно визначає мету та спосіб подальшої обробки, що зближує його статус із самостійним володільцем персональних даних (у термінології законопроекту № 8153 про захист персональних даних, гармонізований із Регламентом (ЄС) 2016/679 [6; 5]). Це суттєво ускладнює здатність адвоката гарантувати клієнту дотримання адвокатської таємниці, оскільки ступінь його контролю після передачі даних залежить від архітектури сервісу та договірних умов провайдера.

Стаття 29 Закону «Про захист персональних даних» допускає транскордонну передачу персональних даних до держави без належного захисту лише за письмової згоди суб'єкта даних [3]; при цьому чинний перелік держав із належним захистом, затверджений Кабінетом Міністрів [4], застосовується виключно для порталу

«Дія» і не є універсальним. Ця норма розрахована на типову передачу даних володільцем бази й не враховує ситуації, коли особа зв'язана додатковим обов'язком нерозголошення, що впливає зі статусу адвоката та користується підвищеним правовим захистом: згода клієнта на обробку персональних даних знімає перешкоду за статтею 29, але автоматично не знімає обмежень статті 22 Закону «Про адвокатуру та адвокатську діяльність» [1], оскільки йдеться про різні за призначенням інститути – правомірність обробки даних і професійний обов'язок адвоката. Законопроект № 8153 [6] спрямований на імплементацію стандартів GDPR та модернізованої Конвенції Ради Європи № 108+ [11] не містить спеціального режиму саме для професійної таємниці, оскільки загальні механізми статей 45–49 GDPR [5] розраховані на типових суб'єктів обробки даних.

Європейський суд з прав людини послідовно визнає адвокатську таємницю фундаментальною гарантією за статтею 8 Convention for the Protection of Human Rights and Fundamental Freedoms [12], яка не є абсолютною, але підлягає обмеженням лише за умови законності, легітимної мети та необхідності в демократичному суспільстві. У справі *Michaud v. France* [13] Суд визнав сумнісним із Конвенцією обов'язок адвокатів повідомляти про підозрілі операції, оскільки регулювання мало достатні гарантії захисту професійної таємниці, – цей підхід можна застосувати й до оцінки допустимості використання адвокатами AI-систем: будь-яке втручання повинно ґрунтуватися на чітких законодавчих підставах, легітимній меті, пропорційності та процесуальних гарантіях. У справі *Reznik v. Ukraine* (2025) [14] Суд, попри зміни законодавства після *Golovan v. Ukraine* [15], дійшов висновку про недостатність процесуальних гарантій захисту адвокатської таємниці під час обшуків і вилучення електронних носіїв [14]. Аналогічну позицію Суд зайняв і у справі *Denysyuk and Others v. Ukraine* (2025) [16], визнавши порушення статті 8 через відсутність у національному законодавстві правил поводження з матеріалами, що випадково потрапили під захист адвокатської таємниці під час негласних слідчих дій, та відсутність незалежного нагляду за такими заходами. У справі *Černý and Others v. the Czech Republic* (2025) [17] Суд наголосив, що захист комунікацій адвоката і клієнта був би позбавлений сенсу, якби не поширювався на електронні дані незалежно від пристрою, на якому вони зберігаються, – вирішальним критерієм є не місце зберігання, а характер інформації та її належність до привілейованих комунікацій. Хоча жодна із цих справ безпосередньо не стосувалася хмарних чи AI-сервісів, системне тлумачення практики Суду, засноване на принципі технологічної нейтральності статті 8 Конвенції, дає підстави поширювати відповідні гарантії і на інформацію, що обробляється в інфраструктурі іноземних провайдерів. У сукупності ця практика свідчить про поступовий перехід Суду від захисту конфіденційності спілкування як такого до захисту цифрового середовища, у якому воно здійснюється.

Рекомендації CCBE прямо поширюють обов'язок збереження адвокатської таємниці на використання генеративних систем ШІ, вимагаючи попередньої оцінки правових підстав обробки даних [8], а *Formal Opinion 512* Американської асоціації юристів – інформованої згоди клієнта, якщо система може використовувати введені дані для донавчання [10]. Хоча ці документи не мають обов'язкової юридичної сили в Україні, вони відображають міжнародні стандарти належної професійної обачності (due diligence) і можуть слугувати орієнтиром для

тлумачення обов'язку конфіденційності за статтею 10 Правил адвокатської етики [2] та статтею 22 Закону «Про адвокатуру та адвокатську діяльність» [1].

Висновки. Проведене дослідження дало змогу встановити, що використання адвокатами хмарних сервісів та інструментів штучного інтелекту іноземних провайдерів актуалізує проблему одночасного застосування двох правових режимів: обов'язку нерозголошення адвокатської таємниці [1; 2], побудованого за суб'єктивним принципом і не поширюваного на технологічних провайдерів, та режиму трансграничної передачі персональних даних [3; 6], побудованого за об'єктивним принципом і не адаптованого до підвищеної суворості професійної таємниці. Вирішення цієї нормативної неузгодженості, на думку автора, доцільно здійснювати із застосуванням принципу *lex specialis derogat generali*. Оскільки правове регулювання адвокатської діяльності встановлює спеціальний режим охорони професійної інформації, який передбачає підвищені гарантії конфіденційності, порівняно із загальним режимом захисту персональних даних, у випадках одночасного застосування цих правових режимів пріоритет має надаватися законодавству про адвокатуру, якщо інше прямо не встановлено законом. Аналіз практики ЄСПЛ [14–17] та рекомендацій ССВЕ і АВА [8–10] підтверджує цей висновок і дає нормативний орієнтир для його реалізації на національному рівні, хоча слід чітко розрізняти де-юре обов'язковий характер практики ЄСПЛ за статтею 8 Конвенції, яка згідно із Законом «Про виконання рішень та застосування практики Європейського суду з прав людини» [18] є джерелом права в Україні, і суто рекомендаційний, де-факто характер стандартів ССВЕ та АВА [8–10], які не зумовлюють самостійних юридичних обов'язків для українських адвокатів, але можуть використовуватися як допоміжний орієнтир під час імплементації відповідних підходів у національне регулювання адвокатської етики.

На підставі проведеного дослідження пропонуються такі напрями вдосконалення законодавства та професійного регулювання.

По-перше, доцільно доповнити статтю 22 Закону «Про адвокатуру та адвокатську діяльність» [1] положенням, яке прямо поширює режим адвокатської таємниці на передачу інформації провайдером хмарних та AI-сервісів, а також обов'язком адвоката здійснювати попередню оцінку ризиків порушення конфіденційності.

По-друге, під час доопрацювання законопроекту про захист персональних даних № 8153 [6] до другого читання, доцільно передбачити спеціальний режим трансграничної передачі даних, пов'язаних із професійною таємницею (адвокатською, нотаріальною, лікарською), з підвищеними гарантіями порівняно зі статтею 29 Закону «Про захист персональних даних» [3].

По-третє, органам адвокатського самоврядування – НААУ та Раді адвокатів України – доцільно розробити рекомендації щодо використання хмарних та AI-сервісів з урахуванням підходів ССВЕ [8; 9] та АВА [10], включно з обов'язком інформованої згоди клієнта, заборобою введення ідентифікуючих даних до загальнодоступних AI-сервісів та перевіркою політики сервісу щодо подальшого використання даних.

По-четверте, у процесі гармонізації законодавства України з правом ЄС доцільно врахувати вимогу AI Act [19] щодо забезпечення грамотності у сфері штучного інтелекту серед осіб, які використовують такі системи, шляхом включення вимог щодо AI literacy до системи підвищення кваліфікації адвокатів.

Перспективи подальших наукових розвідок у цьому напрямі пов'язані з дослідженням впливу виявлених прогалин правового регулювання на забезпечення інших видів професійної таємниці (нотаріальної, лікарської, банківської), проведенням порівняльно-правового аналізу досвіду держав – членів ЄС щодо регулювання використання адвокатами хмарних та AI-сервісів у контексті подальшого розвитку законодавства України (зокрема, законопроекту № 8153), а також опрацюванням критеріїв належної професійної обачності (*due diligence*) адвоката під час вибору й використання AI-інструментів з урахуванням вимог AI Act.

Список використаних джерел

1. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 № 5076-VI. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/5076-17#Text>.
2. Правила адвокатської етики від 09.06.2017 (у ред. від 15.02.2019). *З'їзд адвокатів України*. URL: <https://zakon.rada.gov.ua/rada/show/n0001891-17#Text>.
3. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>.
4. Деякі питання передачі персональних даних за межі України засобами Єдиного державного вебпорталу електронних послуг : постанова Кабінету Міністрів України від 16 серпня 2022 р. № 910. *Кабінет Міністрів України*. URL: <https://zakon.rada.gov.ua/laws/show/910-2022-%D0%BF#Text>.
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). *Official Journal of the European Union*. L 119, 04.05.2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.
6. Проект Закону про захист персональних даних : реєстр. № 8153 від 25.10.2022. *Верховна Рада України*. URL: <https://itd.rada.gov.ua/billInfo/Bills/Card/40707>.
7. Оргинська М. Штучний інтелект: практичні та етичні питання у роботі юриста. *Вища школа адвокатури НААУ*. URL: <https://www.hsa.org.ua/blog/stucnii-intelekt-prakticni-ta-etichni-pitannia-u-roboti-iurista>.
8. CCBE guide on the use of generative AI by lawyers. Brussels : Council of Bars and Law Societies of Europe. 2 October 2025. 28 p. URL: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf.
9. CCBE technical guide on the use of AI tools and models by lawyers. Brussels : Council of Bars and Law Societies of Europe. 27 March 2026. 19 p. URL: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20260327_CCBE-technical-guide-on-the-use-of-AI-tools-and-models-by-lawyers.pdf.
10. Generative Artificial Intelligence Tools. Formal Opinion 512. *American Bar Association. Standing Committee on Ethics and Professional Responsibility*. Chicago, 29 July 2024. 15 p. URL: https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf.

11. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS № 223). Council of Europe, Strasbourg, 10 Oct. 2018. URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=223>.
12. Convention for the Protection of Human Rights and Fundamental Freedoms (ETS № 005) : Council of Europe Convention, Rome, 4 Nov. 1950. URL: <https://rm.coe.int/1680a2353d>.
13. Case of Michaud v. France, European Court of Human Rights (Fifth Section), Application No. 12323/11, Judgment of 6 December 2012. URL: <https://hudoc.echr.coe.int/fre?i=001-115377>.
14. Reznik v. Ukraine, no. 31175/14, Judgment, European Court of Human Rights, 23 January 2025. HUDOC Database. URL: <https://hudoc.echr.coe.int/eng?i=001-240192>.
15. Golovan v. Ukraine, no. 41716/06, Judgment, European Court of Human Rights, 5 July 2012. HUDOC Database. URL: <https://hudoc.echr.coe.int/ukr?i=001-112021>.
16. Denysyuk and Others v. Ukraine, nos. 22790/19 and 3 others, Judgment, European Court of Human Rights, 13 February 2025. HUDOC Database. URL: <https://hudoc.echr.coe.int/eng?i=001-241747>.
17. Černý and Others v. the Czech Republic (Applications nos. 37514/20, 37525/20, 37533/20, 37546/20 and 37555/20): Judgment of the European Court of Human Rights, 18 December 2025. HUDOC Database. URL: <https://hudoc.echr.coe.int/eng?i=001-247564>.
18. Про виконання рішень та застосування практики Європейського суду з прав людини : Закон України від 23.02.2006 № 3477-IV. Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/3477-15#Text>.
19. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008, (EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union. OJ L, 2024/1689, 12.7.2024. URL: <http://data.europa.eu/eli/reg/2024/1689/oj>.

References

1. Verkhovna Rada of Ukraine (2012). Pro advokaturu ta advokatsku diialnist: Zakon Ukrainy vid 05.07.2012 № 5076-VI [On the Bar and Advocacy: Law of Ukraine of 05 July 2012 No. 5076-VI]. Retrieved from <https://zakon.rada.gov.ua/laws/show/5076-17#Text> [in Ukrainian].
2. Pravyla advokatskoi etyky vid 09.06.2017 (u red. vid 15.02.2019) [Rules of Advocate Ethics of 09 June 2017 (as amended on 15 February 2019)]. Zidz advokativ Ukrainy. Retrieved from <https://zakon.rada.gov.ua/rada/show/n0001891-17#Text> [in Ukrainian].
3. Verkhovna Rada of Ukraine (2010). Pro zakhyst personalnykh danykh : Zakon Ukrainy vid 01.06.2010 № 2297-VI [On Personal Data Protection: Law of Ukraine of 01 June 2010 No. 2297-VI]. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].
4. Cabinet of Ministers of Ukraine (2022). Deiaki pytannia peredachi personalnykh danykh za mezhi Ukrainy zasobamy Yedynoho derzhavnoho vebportalu elektronnykh posluh: postanova Kabinetu Ministriv Ukrainy vid 16 serpnia 2022 r. № 910 [Certain Issues of the Transfer of Personal Data Outside Ukraine via the Unified State Web Portal of Electronic Services: Resolution of the Cabinet of Ministers of Ukraine of 16 August 2022 No. 910]. Retrieved from <https://zakon.rada.gov.ua/laws/show/910-2022-n#Text> [in Ukrainian].
5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union. L 119, 04.05.2016. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng> [in English].
6. Verkhovna Rada of Ukraine (2022). Proiekt Zakonu pro zakhyst personalnykh danykh : reiestr. № 8153 vid 25.10.2022 [Draft Law on Personal Data Protection: Reg. No. 8153 of 25 October 2022]. Retrieved from <https://itd.rada.gov.ua/billInfo/Bills/Card/40707> [in Ukrainian].
7. Ortynska, M. Shtuchnyi intelekt: praktychni ta etychni pytannia u roboti yurysta [Artificial Intelligence: Practical and Ethical Issues in a Lawyer's Work]. Vyshcha shkola advokatury NAAU. Retrieved from <https://www.hsa.org.ua/blog/stucnii-in-telekt-praktychni-ta-etichni-pytannia-u-roboti-iurista> [in Ukrainian].
8. CCBE guide on the use of generative AI by lawyers. Brussels: Council of Bars and Law Societies of Europe, 2 October 2025. 28 p. Retrieved from https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf [in English].
9. CCBE technical guide on the use of AI tools and models by lawyers. Brussels: Council of Bars and Law Societies of Europe, 27 March 2026. 19 p. Retrieved from https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20260327_CCBE-technical-guide-on-the-use-of-AI-tools-and-models-by-lawyers.pdf [in English].
10. Generative Artificial Intelligence Tools. Formal Opinion 512. American Bar Association. Standing Committee on Ethics and Professional Responsibility. Chicago, 29 July 2024. 15 p. Retrieved from https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf [in English].
11. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Council of Europe, Strasbourg, 10 Oct. 2018. Retrieved from <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treaty-num=223> [in English].
12. Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 005): Council of Europe Convention, Rome, 4 Nov. 1950. Retrieved from <https://rm.coe.int/1680a2353d> [in English].
13. Case of Michaud v. France, European Court of Human Rights (Fifth Section), Application No. 12323/11, Judgment of 6 December 2012. Retrieved from <https://hudoc.echr.coe.int/fre?i=001-115377> [in English].
14. Reznik v. Ukraine, no. 31175/14, Judgment, European Court of Human Rights, 23 January 2025. HUDOC Database. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-240192> [in English].

15. Golovan v. Ukraine, no. 41716/06, Judgment, European Court of Human Rights, 5 July 2012. HUDOC Database. Retrieved from <https://hudoc.echr.coe.int/ukr?i=001-112021> [in English].
16. Denysyuk and Others v. Ukraine, nos. 22790/19 and 3 others, Judgment, European Court of Human Rights, 13 February 2025. HUDOC Database. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-241747> [in English].
17. Černý and Others v. the Czech Republic (Applications nos. 37514/20, 37525/20, 37533/20, 37546/20 and 37555/20): Judgment of the European Court of Human Rights, 18 December 2025. HUDOC Database. Retrieved from <https://hudoc.echr.coe.int/eng?i=001-247564> [in English].
18. Verkhovna Rada of Ukraine (2006). Pro vykonannya rishen ta zastosuvannya praktyky Yevropeiskoho sudu z prav liudyny: Zakon Ukrainy vid 23.02.2006 № 3477-IV [On the Execution of Judgments and Application of the Case Law of the European Court of Human Rights: Law of Ukraine of 23 February 2006 No. 3477-IV]. Retrieved from <https://zakon.rada.gov.ua/laws/show/3477-15#Text> [in Ukrainian].
19. 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). *Official Journal of the European Union*. OJ L, 2024/1689, 12.7.2024. Retrieved from <http://data.europa.eu/eli/reg/2024/1689/oj> [in English].

Telychko Oksana,

Candidate of Law, Associate Professor,
Head of the Department of Law

(State University of Economics and Technology, Kryvyi Rih)

ORCID: <https://orcid.org/0000-0003-2536-7442>

Rekun Viktor,

Candidate of Law, Associate Professor,
Associate Professor at the Department of Law

(State University of Economics and Technology, Kryvyi Rih)

ORCID: <https://orcid.org/0000-0002-2636-9426>

LEGAL REGULATION OF ATTORNEY-CLIENT PRIVILEGE IN THE CONTEXT OF CLOUD SERVICES AND ARTIFICIAL INTELLIGENCE SYSTEMS

The article examines the legal protection of attorney-client privilege in the context of the digitalization of legal activities caused by the use of cloud services and artificial intelligence systems by attorneys. It is substantiated that the use of foreign digital platforms in the process of a lawyer's professional activity creates risks for the confidentiality of information about clients due to the possible cross-border transfer of personal data and access to them by technology providers. It is established that the legislation of Ukraine does not contain special legal regulation of the use of cloud services and artificial intelligence systems by attorneys and does not determine the specifics of the relationship between the obligation to observe attorney-client privilege and the regime for the protection of personal data during their cross-border transfer.

*The provisions of the legislation of Ukraine, Regulation (EU) 2016/679 (GDPR), the practice of the European Court of Human Rights, the recommendations of the Council of Bars and Law Societies of Europe (CCBE) and the American Bar Association (ABA) are analyzed. It is proven that the use of foreign cloud and AI services actualizes the problem of simultaneous application of the attorney-client privilege regime and personal data protection. The existence of a regulatory inconsistency between the provisions of the legislation is substantiated and a mechanism for overcoming it is proposed by applying the principle of *lex specialis derogat generali*.*

It is proposed to improve national legislation by extending special guarantees of attorney-client privilege to the use of digital services, introducing a special regime for cross-border transfer of information constituting a professional secret, and developing professional recommendations for the safe use of artificial intelligence technologies in advocacy. It is concluded that effective protection of attorney-client privilege requires the adaptation of traditional legal mechanisms to the modern digital environment, taking into account European standards for the protection of human rights.

Key words: attorney-client privilege, cloud services, artificial intelligence, personal data protection, cross-border data transfers, confidentiality, European Court of Human Rights.



Дата першого надходження статті до видання: 09.07.2026
Дата прийняття статті до друку після рецензування: 05.08.2026
Дата публікації (оприлюднення) статті: 15.10.2026