УДК 341.231.14:004.738.5
DOI: https://doi.org/10.24144/2307-3322.2026.94.4.39

ЦИФРОВІ ПРАВА ЛЮДИНИ У СИСТЕМІ ЄКПЛ: ДОКТРИНАЛЬНІ ПІДХОДИ ДО НОВИХ ВИКЛИКІВ

Васильчук Л.Б.,
кандидат юридичних наук, доцент, доцент
кафедри конституційного права
та порівняльного правознавства
ДВНЗ «Ужгородський національний університет»
ORCID: 0009-0006-2527-7337

Васильчук Л.Б. Цифрові права людини у системі ЄКПЛ: доктринальні підходи до нових викликів.

Стаття присвячена дослідженню доктринальних підходів до формування та захисту цифрових прав людини у системі Європейської конвенції про захист прав людини і основоположних свобод (ЄКПЛ). Встановлено, що цифрові права не становлять самостійної нормативної категорії ЄКПЛ, однак практика ЄСПЛ виробила механізм їх динамічного захисту через розширювальне тлумачення класичних прав, передусім статей 8 і 10 Конвенції. Досліджено доктринальні засади захисту права на приватне життя у цифровому середовищі на прикладі справ щодо масового спостереження, блокування інтернету та шифрування комунікацій. Проаналізовано прецедентну практику ЄСПЛ у справах щодо наскрізного шифрування та масового перехоплення комунікацій, що визначили сучасний стандарт цифрового захисту. Розглянуто доктрину «живого інструменту» та «поля розсуду держав» як методологічну основу адаптації ЄКПЛ до цифрової реальності. Виявлено, що ЄСПЛ виробив специфічні критерії оцінювання цифрових обмежень прав: принцип законності (передбачуваності і доступності закону), принцип необхідності в демократичному суспільстві та принцип пропорційності. Окрему увагу приділено позитивним зобов'язанням держав у цифровій сфері, зокрема обов'язку забезпечити правову базу для захисту персональних даних та свободи онлайн-вираження. Зроблено висновок, що ефективний захист цифрових прав у системі ЄКПЛ вимагає подальшого розвитку як конвенційної доктрини, так і національного законодавства держав-учасниць.

Ключові слова: цифрові права, ЄКПЛ, право на приватне життя, свобода вираження поглядів онлайн, наскрізне шифрування, масове спостереження, позитивні зобов'язання держав.

Vasylchuk L.B. Digital human rights in the ECHR system: doctrinal approaches to new challenges.

The article examines the doctrinal approaches to the formation and protection of digital human rights within the system of the European Convention on Human Rights and Fundamental Freedoms (ECHR). It is established that digital rights do not constitute an independent normative category of the ECHR; however, the ECtHR's case law has developed a mechanism for their dynamic protection through an expansive interpretation of classical rights, primarily Articles 8 and 10 of the Convention. The doctrinal foundations of the protection of the right to private life in the digital environment are examined through the lens of cases concerning mass surveillance, internet blocking, and the encryption of communications. The ECtHR's case law in cases concerning end-to-end encryption (Podchasov v. Russia, 2024) and bulk interception of communications (Big Brother Watch v. UK, 2021) is analysed, identifying the current standard of digital protection under the Convention. The living instrument doctrine and the doctrine of the margin of appreciation are considered as the methodological basis for the adaptation of the ECHR to digital reality. It is established that the ECtHR has developed specific criteria for assessing digital restrictions of rights: the principle of legality (foreseeability and accessibility of the law), the principle of necessity in a democratic society, and the principle of proportionality. Special attention is paid to states' positive obligations in the digital sphere, in particular the duty to establish a legal framework for the protection of personal data and freedom of online expression. It is concluded that effective protection of digital rights in the ECHR system requires further development of both the Convention doctrine and the national legislation of the Member States. The study contributes to the ongoing scholarly debate on

the sufficiency of the classical human rights framework for responding to the challenges of the digital age and proposes criteria for assessing the quality of domestic legal regulation of digital rights.

Key words: digital rights, ECHR, right to private life, freedom of online expression, end-to-end encryption, mass surveillance, positive obligations of states.

Постановка проблеми. Цифрова трансформація суспільства поставила перед системою захисту прав людини виклики, які її творці у 1950 р. не могли передбачити. Право на повагу до приватного листування (стаття 8 ЄКПЛ) сьогодні *de facto* охоплює мільярди зашифрованих повідомлень та хмарні сховища персональних даних; свобода вираження поглядів (стаття 10 ЄКПЛ) реалізується передусім через цифрові платформи, алгоритми яких визначають видимість контенту; право на ефективний засіб правового захисту (стаття 13 ЄКПЛ) стикається з непрозорістю автоматизованих рішень, що визначають доступ до інформації та правосуддя.

Гострота проблеми, на нашу думку, в першу чергу визначається кількома взаємопов'язаними факторами. Так, по-перше, темп технологічних змін принципово перевищує темп нормотворчості: законодавець завжди перебуває в ролі наздоганяючого. По-друге, цифрові загрози правам людини мають транскордонний й асиметричний характер, вони однаково виходять від держав через системи масового стеження і від транснаціональних платформ через непрозорі алгоритми модерації. По-третє, традиційні конвенційні конструкції (в т.ч. «законність», «необхідність» і «пропорційність»), вимагають переосмислення у контексті технологій, де «закон» може бути технічним стандартом, а «пропорційність» - неможливою для оцінки без спеціальних технічних знань.

Сама ЄКПЛ залишилася текстуально незмінною. Відповідь на виклик забезпечили не конвенційні поправки, а доктринальна еволюція – насамперед практика ЄСПЛ, що через доктрину «живого інструменту» поступово сформувала систему захисту цифрових прав. Це доктринальне досягнення є вражаючим, однак породжує власні запитання: де межа між тлумаченням і нормотворчістю? Чи не настав час для системної конвенційної реформи у сфері цифрових прав?

Аналіз останніх досліджень. Насамперед звернемося до іноземних джерел. Так, у зарубіжній доктрині питання цифрових прав у системі ЄКПЛ досліджується у кількох взаємопов'язаних напрямах. Перший – конвенційний захист наскрізного шифрування: Дж. Шурсон аналізує, чи встановлює ЄКПЛ право на наскрізне шифрування на підставі рішення ЄСПЛ у справі Podchasov v. Russia [1]; М. Пірзада досліджує це рішення як новий вектор у «крипто-війнах» [5]. Другий – масове спостереження: М. Зальнерюте виявляє, що ЄСПЛ у справі Big Brother Watch v. UK легітимізував масове спостереження через підхід «процедурного фетишизму» [3]; спільний довідник ЄСПЛ та FRA систематизує взаємодію практики ЄСПЛ та справедливості у цій сфері [8]. Третій – доктринальні засади тлумачення ЄКПЛ: П. Коміті обстоює, що доктрини поля розсуду і еволютивного тлумачення є оптимальними канонами тлумачення Конвенції [2]; А. В. Баке досліджує ефективність доктрини позитивних зобов'язань у захисті прав у державах-членах ЄС [4]. Практику ЄСПЛ щодо доступу до інтернету та нових технологій узагальнено у офіційних тематичних довідниках Суду [6; 7].

Серед вітчизняних дослідників слід виокремити такі праці. Д.М. Бєлов, М.В. Бєлова, І.Є. Переш, К.К. Мегеш та І. Покорба розробляють доктринальні засади цифрових прав людини, наголошуючи на відсутності чіткого нормативного визначення цього поняття та необхідності вдосконалення правових рамок, досліджують право людини на забуття як один із ключових цифрових прав у системі ЄКПЛ [10; 11; 14]. В.А. Бочковой та Н.А. Бааджи аналізують обмеження цифрових прав в умовах сучасних правових викликів, включаючи практику ЄСПЛ [12]. К. С. Тверезовська систематизує поняття, види та значення цифрових прав людини [13].

Метою статті є дослідження окремих доктринальних підходів ЄСПЛ до захисту цифрових прав людини крізь призму статей 8 і 10 ЄКПЛ, аналіз ключових прецедентів та виявлення теоретико-правових засад для удосконалення вітчизняного законодавства у цій сфері.

Виклад матеріалу дослідження. Відправною точкою аналізу захисту цифрових прав за ЄКПЛ є доктрина «живого інструменту» *(living instrument doctrine)*, вперше сформульована у справі Tyrer v. United Kingdom (1978). Суть цієї доктрини полягає в тому, що ЄКПЛ є живим інструментом, що підлягає тлумаченню у світлі сучасних умов, а не виключно відповідно до намірів її засновників. Саме ця доктрина уможливила охоплення конвенційними статтями цілих сфер суспільного життя, що не існували на момент підписання Конвенції у 1950 р.

П. Коміті у своєму дослідженні виявляє, що доктрини поля розсуду й еволютивного тлумачення є взаємопов'язаними і взаємодоповнювальними канонами тлумачення ЄКПЛ. Дослідник стверджує, що, попри критику цих доктрин як позбавлених нормативного підґрунтя і таких, що є суддівськими конструктами, вони відповідають правилам тлумачення договорів за Віденською конвенцією про право міжнародних договорів і є найоптимальнішими інструментами для динамічного застосування ЄКПЛ в умовах постійно змінюваного світу [2]. Там само автор зазначає, що оскільки тлумачення та застосування законів здійснюється у постійно змінюваному світі, який вимагає динамічних законів, здатних адаптуватися до нових ситуативних контекстів, доктрина живого інструменту є концептуально необхідною, а не лише зручною.

У цифровому контексті доктрина живого інструменту забезпечила кілька ключових розширень конвенційного захисту. По-перше, поширення статті 8 на електронну кореспонденцію, метадані і зашифровані повідомлення. По-друге, охоплення статтею 10 інтернету як «одного з основних засобів, через який особи реалізують своє право на свободу вираження поглядів та отримання інформації» (Ahmet Yıldırım v. Turkey, 2012). По-третє, вироблення стандартів законності, необхідності та пропорційності цифрових обмежень, адаптованих до технологічних реалій.

Як бачимо, доктрина живого інструменту є не просто судовою технікою, а доктринальним вибором, що відображає концепцію ЄКПЛ як конституційного документа європейського публічного правопорядку. Її застосування у цифровій сфері є неминучим, проте воно ставить перед дослідниками питання про межі суддівської правотворчості та необхідність більш системної нормотворчої відповіді на цифрові виклики.

Власне саме стаття 8 ЄКПЛ, що гарантує право на повагу до приватного та сімейного життя, житла і кореспонденції, є центральним конвенційним механізмом захисту цифрової приватності. Практика ЄСПЛ виробила розгалужену систему стандартів щодо трьох основних категорій цифрових порушень: масового перехоплення комунікацій, зберігання метаданих та вимог до розшифрування.

У справі Big Brother Watch and Others v. UK (Grand Chamber, 2021) ЄСПЛ вперше безпосередньо оцінив режим масового перехоплення комунікацій після викриттів Сноудена. М. Зальнерюте, аналізуючи цей прецедент, встановлює, що Велика палата обрала підхід «процедурного фетишизму»: замість того щоб визнати масове перехоплення несумісним з ЄКПЛ за своєю суттю, Суд задовольнився наявністю формальних процедурних гарантій: незалежного нагляду, обмежень на використання та систем видалення даних [3]. Там само дослідниця зазначає, що три судді з окремими думками охарактеризували це як упущену можливість захистити електронний «Великий брат» в Європі.

Принципово новий вектор у захисті цифрової приватності визначила справа Podchasov v. Russia (ECtHR, 13 лютого 2024 р., заява № 33696/19), що встановила загальнообов'язковий для держав-учасниць ЄКПЛ стандарт щодо законодавчих вимог розшифрування зашифрованих комунікацій. Суд вперше у своїй практиці безпосередньо оцінив законність таких вимог. Показово, що ще до цього рішення Суд справедливості ЄС у справах Digital Rights Ireland (C-293/12, 2014) та La Quadrature du Net (C-511/18, 2020) визнав несумісним із Хартією основних прав ЄС як масове збереження метаданих, так і зобов'язання щодо розшифрування. Таким чином, ЄСПЛ підтвердив та поглибив стандарт, що вже існував у праві ЄС. Дж. Шурсон, аналізуючи це рішення, встановлює, що ЄСПЛ одноголосно констатував порушення статті 8, оскільки законодавча вимога до «організаторів поширення інформації» надавати ключі шифрування становила непропорційне втручання у право на приватне життя, адже доступні технічні засоби дешифрування неминуче послаблюють безпеку комунікацій усіх користувачів сервісу [1]. Там само авторка підкреслює, що це рішення є вагомим прецедентом для держав (зокрема Великої Британії та ЄС), що розглядають аналогічні зобов'язання щодо розшифрування.

Окремо звернемося до доктрини позитивних зобов'язань держав у цифровій сфері. А.В. Баке у своєму дослідженні доктрини позитивних зобов'язань ЄКПЛ виявляє, що ця доктрина не може бути механічно перенесена до права ЄС, оскільки різними принципами керуються ці правові режими захисту фундаментальних прав [4]. Там само дослідниця встановлює, що стосовно процесуальних зобов'язань ЄСПЛ схильний відмовляти від поля розсуду держав, тоді як право ЄС принципово ширше залишає простір для процесуальної автономії держав-членів.

Стаття 10 ЄКПЛ, гарантуючи свободу вираження поглядів і отримання інформації, є другим ключовим конвенційним механізмом захисту цифрових прав. Її практичне значення у цифровому

середовищі виявляється у трьох основних напрямах: захист від блокування інтернету та цензури онлайн-контенту; захист права доступу до достовірної публічної інформації; захист конфіденційності комунікацій журналістів.

Довідник ЄСПЛ з практики щодо доступу до інтернету та свободи отримання і поширення інформації фіксує стандарт, відповідно до якого заходи, що обмежують доступ до інтернету, визнаються Судом порушенням статті 10, якщо наслідки відповідного заходу є свавільними, а судовий контроль є недостатнім для запобігання зловживанням [6]. Показовими є справи щодо Туреччини, де органи влади систематично вдавалися до блокування значних масивів інтернет-контенту без достатнього правового підґрунтя.

Важливим аспектом цифрового виміру статті 10 є право доступу до достовірної інформації. У справі Association Burestop 55 and Others v. France ЄСПЛ вперше визнав, що право доступу до інформації за статтею 10 обов'язково охоплює якісний аспект – вимогу до того, щоб розкрита інформація була щирою, точною, достатньою та достовірною. Це рішення може мати далекосяжні наслідки для регулювання цифрового інформаційного середовища в умовах «постправди» [8].

Взаємодія статей 8 і 10 у контексті захисту журналістських комунікацій є особливо значущою. Рада Ради Європи щодо конфіденційності і захисту персональних даних підкреслює, що ЄСПЛ поширив позитивне зобов'язання за статтею 8 щодо перехоплення комунікацій на журналістів, застосовуючи підвищені процесуальні й матеріальні гарантії в тих справах, де стеження мало навмисний вплив на журналістські джерела [8]. Масовий збір даних, що побічно зачіпає журналістські комунікації, також потрапляє в орбіту посиленого захисту.

Цифровий вимір статті 10 демонструє принципову закономірність: ЄСПЛ послідовно вимагає, щоб цифрові обмеження свободи вираження поглядів відповідали тим самим критеріям законності, необхідності та пропорційності, що й аналогові. Разом з тим технологічна специфіка цифрових обмежень, мережеві ефекти блокувань, непропорційний вплив на невинних користувачів, вимагає адаптованого застосування цих критеріїв, що Суд і здійснює в рамках доктрини живого інструменту.

Доктрина поля розсуду держав *(margin of appreciation)* є одним з найважливіших інструментів балансування між захистом прав людини і суверенними повноваженнями держав у системі ЄКПЛ. У цифровому контексті вона набуває особливої ваги через швидкість технологічних змін, що унеможливлює повну уніфікацію регуляторних підходів на конвенційному рівні.

П. Коміті наголошує, що попри внесення доктрини поля розсуду до Протоколу № 15 (2013) як «невід'ємного і постійного явища за Конвенцією», необхідні «принципові критерії» для її застосування [2]. Відсутність таких критеріїв у цифровій сфері є системною прогалиною, що породжує непередбачуваність для держав, бізнесу та індивідуальних суб'єктів.

У практиці ЄСПЛ щодо масового спостереження поле розсуду є звуженим. Практика Ради Європи фіксує, що ключовими стандартами законності масового перехоплення комунікацій є: передбачуваність закону; наявність незалежного авторизаційного органу; наявність незалежного наглядового органу; наявність ефективних засобів правового захисту для осіб, що зазнали стеження [8]. У справі Big Brother Watch Велика палата підтвердила, що режим масового перехоплення не виключається Конвенцією за умови дотримання цих критеріїв. М. Зальнерюте, проте, звертає увагу на те, що такий підхід фактично нормалізує масове спостереження, надаючи йому «процедурний паспорт» навіть за умови системного охоплення усіх користувачів [3].

У справах про шифрування поле розсуду є іще вужчим. Дж. Шурсон встановлює, що ЄСПЛ в рішенні у справі Podchasov v. Russia не залишив державі поля розсуду щодо вибору між наскрізним шифруванням та «бекдорами»: оскільки будь-який технічний механізм дешифрування об'єктивно погіршує безпеку комунікацій усіх користувачів, а не лише тих, за ким ведеться стеження, відповідний законодавчий захід є непропорційним незалежно від будь-яких правових гарантій [1].

Як бачимо, доктрина поля розсуду у цифровому контексті є не інструментом ліберальності, а механізмом диференціації залежно від тяжкості втручання: чим більше охоплення стеження, чим глибше воно проникає у зміст комунікацій, тим менше простору для дискреції залишається у держав. Наскрізне шифрування знаходиться у захищеному ядрі конвенційного права, де поле розсуду зведено до нуля.

Поряд із негативними зобов'язаннями (утримуватися від втручання у цифрові права) ЄКПЛ покладає на держав-учасниць позитивні зобов'язання щодо забезпечення реального та ефектив-

ного захисту цих прав. У цифровій сфері позитивні зобов'язання охоплюють кілька ключових напрямів.

Перший – законодавче регулювання захисту персональних даних. Рада Ради Європи наголошує, що ЄКПЛ вимагає наявності у державах-учасницях законодавства, що забезпечує захист персональних даних відповідно до стандартів Конвенції 108 та ЄКПЛ [8]. Це зобов'язання є особливо актуальним для України, яка імплементує GDPR у рамках євроінтеграційного процесу.

Другий – забезпечення ефективних засобів правового захисту від цифрового стеження. Стандарти ЄСПЛ вимагають, щоб особа, якій може бути заподіяно шкоду внаслідок таємного стеження, мала доступ до національних органів оскарження. А. В. Баке у своєму дослідженні встановлює, що саме у сфері процесуальних зобов'язань ЄСПЛ найбільш послідовно відмовляє державам у широкому полі розсуду, вимагаючи наявності конкретних інституційних гарантій [4].

Третій – захист від приватних суб'єктів у цифровому середовищі. Навчально-методичний комплекс Media Defence підкреслює, що зобов'язання держав за ЄКПЛ щодо захисту права онлайн-користувачів поширюється також на створення регуляторного середовища, яке запобігає порушенням цих прав з боку платформ і приватних компаній [9]. Це горизонтальний вимір позитивних зобов'язань, що набуває особливої ваги в умовах домінування великих технологічних компаній.

Четвертий – забезпечення цифрової доступності та права доступу до інтернету. Хоча ЄКПЛ не закріплює автономного права доступу до інтернету, ЄСПЛ через статтю 10 послідовно встановлює, що держави зобов'язані утримуватися від непропорційних блокувань і забезпечувати реальний доступ до засобів цифрової комунікації, необхідних для реалізації прав [6].

Отже, позитивні зобов'язання у цифровій сфері є не менш вагомими за негативні, хоча й складніше піддаються конкретизації. Їхній розвиток у практиці ЄСПЛ вказує на принципову позицію: держава несе відповідальність за стан цифрового правового середовища в цілому, а не лише за власні прямі втручання.

Висновки. За результатами проведеного дослідження можна сформулювати такі висновки:

1. Цифрові права людини не становлять самостійної нормативної категорії ЄКПЛ, проте розвиток практики ЄСПЛ фактично сформував систему їхнього договірного захисту через динамічне тлумачення класичних прав, передусім статей 8 і 10 Конвенції. Доктрина «живого інструменту», підкріплена принципом пропорційності та позитивними зобов'язаннями, є доктринальною основою цього захисту.

2. Справа Podchasov v. Russia (2024) є рубіжним прецедентом, що вперше прямо поширює захист статті 8 ЄКПЛ на наскрізне шифрування комунікацій. Незважаючи на те що держава-відповідач вибула зі складу Ради Європи, сформульований у цьому рішенні стандарт, будь-який технічний механізм «бекдору» непропорційно погіршує безпеку всіх користувачів, а тому є несумісним з Конвенцією незалежно від обсягу процедурних гарантій, є обов'язковим орієнтиром для всіх держав-учасниць ЄКПЛ, включаючи Україну, і суттєво обмежує простір для аналогічних законодавчих ініціатив.

3. Справа Big Brother Watch v. UK (2021) демонструє доктринальну тенденцію «процедурного фетишизму»: ЄСПЛ визнав масове перехоплення сумісним з ЄКПЛ за умови наявності системи формальних гарантій, не оцінюючи його несумісність з Конвенцією за своєю суттю. Ця тенденція є доктринально суперечливою і вимагає подальшої уваги з боку ЄСПЛ та юридичної спільноти.

4. Доктрина поля розсуду держав у цифровій сфері має диференційований характер: вона є найвужчою у випадках втручання в сутнісне ядро права на приватне листування (шифрування) і дещо ширшою щодо режимів масового спостереження за умови дотримання процедурних гарантій. Сам принцип диференціації є правильним, проте Суду необхідно виробити більш чіткі критерії для його застосування у технологічно складних справах.

5. Ефективний захист цифрових прав за ЄКПЛ вимагає від держав-учасниць виконання як негативних (утримання від непропорційних обмежень), так і позитивних (нормативне забезпечення цифрової приватності, ефективні засоби правового захисту, регулювання платформ) зобов'язань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Shurson J. A European right to end-to-end encryption? *Computer Law and Security Review.* 2024. Vol. 55. Art. 106063. DOI: https://doi.org/10.1016/j.clsr.2024.106063. URL: https://www.sciencedirect.com/science/article/pii/S0267364924001298.

2. Komiti P. The doctrines of margin of appreciation and evolutive interpretation: a review of the European Court of Human Rights. SSRN Working Paper. 2023. DOI: https://doi.org/10.2139/ssrn.4885633. URL: https://ssrn.com/abstract=4885633.
3. Zalnieriute M. Procedural fetishism and mass surveillance under the ECHR: Big Brother Watch v. UK. Verfassungsblog. 2021. DOI: https://doi.org/10.17176/20210602-123858-0. URL: https://verfassungsblog.de/big-b-v-uk.
4. Backé A. V. The positive obligations doctrine: a means of effective fundamental rights protection in EU Member States? *Maastricht Journal of European and Comparative Law*. 2024. Vol. 31. No. 4. P. 389–408. DOI: https://doi.org/10.1177/1023263X241268874. URL: https://journals.sagepub.com/doi/10.1177/1023263X241268874.
5. Pirzada M.S.A. Championing digital sovereignty – ECtHR's ruling in Podchasov v. Russia. Georgetown Journal of International Law Blog. 2024. URL: https://www.law.georgetown.edu/international-law-journal/blog/championing-digital-sovereignty-ecthrs-ruling-in-podchasov-v-russia.
6. European Court of Human Rights. Factsheet – Access to internet and freedom to receive and impart information and ideas. Strasbourg: Council of Europe, June 2024. URL: https://www.echr.coe.int/documents/d/echr/FS_Access_Internet_ENG.
7. European Court of Human Rights. Factsheet – New technologies. Strasbourg: Council of Europe, October 2024. URL: https://www.echr.coe.int/documents/d/echr/fs_new_technologies_eng.
8. European Court of Human Rights; European Union Agency for Fundamental Rights. Joint Factsheet – Mass surveillance: ECtHR and CJEU Case-Law. Strasbourg: Council of Europe, 2025. URL: https://ks.echr.coe.int/documents/d/echr-ks/mass-surveillance.
9. Media Legal Defence Initiative. Modules on digital rights and freedom of expression online in Europe. Module 1: Digital rights and emerging challenges. London: Media Legal Defence Initiative, May 2024. ISBN 978-0-9935214-1-6. URL: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2024/06/Modules-on-Digital-Rights-and-Freedom-of-Expression-Online-in-Europe-2024.pdf.
10. Бєлов Д.М., Переш І.Є., Покорба І. Цифрові права людини: доктринальні засади. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 110–115. URL: http://nbuv.gov.ua/UJRN/anpopr_2024_2_19.
11. Бєлова М.В., Бєлов О.М., Мегеш К.К. Право людини на забуття: окремі концептуальні питання. *Аналітично-порівняльне правознавство*. 2024. № 2. С. 116–120. URL: https://journal-app.uzhnu.edu.ua/article/view/303018.
12. Бочковой В.А., Бааджі Н.А. Обмеження цифрових прав людини в умовах сучасних правових викликів. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. Вип. 84. DOI: https://doi.org/10.24144/2307-3322.2024.84.4.31.
13. Тверезовська К.С. Поняття, види та значення цифрових прав людини. *Юридичний науковий електронний журнал*. 2024. № 6. DOI: https://doi.org/10.32782/2524-0374/2024-6/119.
14. Бєлова М.В., Бєлов Д.М. Імплементація штучного інтелекту в досудове розслідування кримінальних справ: міжнародний досвід. *Аналітично-порівняльне правознавство*. 2023. № 2. С. 448–454. URL: https://journal-app.uzhnu.edu.ua/article/view/282310.

Дата першого надходження рукопису до видання: 12.03.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026