https://doi.org/10.26565/2075-1834-2025-39-19
УДК 347.412.1

М. В. ГУРА
кандидат юридичних наук,
старший викладач кафедри цивільно-правових дисциплін
E-mail: m.gura@karazin.ua ORCID: https://orcid.org/0000-0002-7695-7672
Харківський національний університет імені В.Н. Каразіна
м. Харків, 61022, майдан Свободи, 4

ЗНАЧЕННЯ СУДОВОЇ ПРАКТИКИ ЄСПЛ ДЛЯ ІТ-ПРАВА

АННОТАЦІЯ. *Вступ.* Стрімкий прогрес інформаційних технологій та їх поширення у всі сфери життя змушує безупинно вдосконалювати правове регулювання сфери ІТ. В Україні цей процес ускладнюється необхідністю приведення національного законодавства у відповідність до європейських норм, зокрема до практики Європейського суду з прав людини (ЄСПЛ).

Зміст. У статті аналізуються окремі рішення ЄСПЛ щодо різних аспектів ІТ-права: право на приватність в інформаційну епоху (S. and Marper v. The United Kingdom, Kopp v. Switzerland, Roman Zakharov v. Russia), свобода висловлювання в мережі (Ahmet Yildirim v. Turkey, Delfi AS v. Estonia), право на отримання інформації (Ukraine v. Russia (re Crime)) та інші.

Висновки. Автор зазначив, що рішення ЄСПЛ мають розумний вплив на українське законодавство щодо захисту персональних даних, цензури, свободи слова в Інтернеті та відповідальності провайдерів за розміщений контент, а також сприяють розвитку культури прав людини. Дослідник акцентував увагу на наявності галузевих викликів та шляхах їх вирішення.

КЛЮЧОВІ СЛОВА: *Європейський суд з прав людини, ЄСПЛ, ІТ-право, Європейська Конвенція з прав людини, право на приватність, свобода вираження поглядів, доступ до інформації, захист персональних даних.*.

Як цитувати: Гура М. В. Значення судової практики єспл для it-права. *Вісник Харківського національного університету імені В. Н. Каразіна, серія «Право».* 2025. Вип. 39. С.194-201 https://doi.org/10.26565/2075-1834-2025-39-19

In cites: M.V.Hura (2025). The significance of the ECHR case law for IT law. *The Journal of V.N. Karazin National University, Series "Law"*, (39), P. 194-201 https://doi.org/10.26565/2075-1834-2025-39-19 (in Ukrainian)

Постановка проблеми. Дослідження присвячено аналізу впливу рішень ЄСПЛ на ІТ-право, з акцентом на їх роль в Україні. Європейська Конвенція з прав людини (далі – ЄКПЛ) має вирішальне значення для розробки фундаментальних правових змін у таких сферах, як захист даних, свобода вираження думок в Інтернеті та доступ до інформації, що допомагає посилити захист основних прав у цифровому середовищі. Проте дотримання судової практики ЄСПЛ характеризується низкою проблем, зокрема, прогалинами в реалізації та імплементації рішень, необхідність пристосування до нових технологій і необхідність врахування прав та інтересів різних учасників правовідносин, як приватних, так і публічних. Україна зробила значні кроки у приведенні свого законодавства про інформаційні технології у відповідність до стандартів ЄС та норм ЄКПЛ, але нагальною залишається необхідність покращення сфері політики та законодавства для ефективного впровадження актуальних норм та подолання нових викликів. **Стан наукового дослідження теми**. Окремі питання проблематики ІТ-права та впливу рішень ЄСПЛ досліджували О. Гиляк, М. Гнатовський, І. Жаровська, Ю. Іоффе, О. Петришин, Л. Спицька, О. Туазон, Т. Худолій, С. Четрі та інших.

Формулювання мети статті (постановка завдання). Визначити вплив та значення судової практики ЄСПЛ для ІТ-права, з акцентом на їх роль в Україні.

Матеріали та методи. Для проведення дослідження застосовувались загально-наукові та спеціально-наукові методи. Загальнонаукові методи: 1) аналіз та синтез: дозволили розчленувати проблему на складові частини (аналіз рішень ЄСПЛ, законодавства України, наукових джерел) та об'єднати отримані результати та структурувати дослідження; 2) індукція та дедукція: застосовано для виявлення закономірностей на основі аналізу рішень ЄСПЛ та формулювання

висновків щодо впливу цих рішень на ІТ-право;3) порівняння: дозволило зіставити правові норми та практики України з положеннями ЄКПЛ та рішеннями ЄСПЛ, виявити подібності та відмінності; 4) абстрагування: допомогло виділити суттєві характеристики досліджуваних явищ

Спеціально-наукові методи: 1) формально-догматичний метод: використано для аналізу правових норм, що містяться в ЄКПЛ, рішеннях ЄСПЛ та законодавстві України, з метою виявлення їх змісту, структури та взаємозв'язку; 2) герменевтичний метод: застосовано для тлумачення правових текстів, зокрема рішень ЄСПЛ, з урахуванням контексту, мети та обставин їх прийняття. Матеріали дослідження: міжнародно-правові акти, національне законодавство, рішення ЄСПЛ, наукова література.

Виклад основного матеріалу. Необхідність розвитку ІТ-права в Україні набуває все більшої актуальності, особливо з огляду на появу нових технологій та необхідності гармонізації українського законодавства зі стандартами ЄС. ІТ-право має важливе значення для приватних та публічних правовідносин, зокрема у питаннях електронного урядування як фактору удосконалення функціонування публічної влади в постволенний період [1, с. 158].

Рішення ЄСПЛ є джерелом національного права багатьох країн та є обов'язковими для виконання всіма державами-учасницями Європейської Конвенції з прав людини, що прямо передбачено у ст. 46 ЄКПЛ.

Додатково дана вимога закріплена у національних нормативних актах, зокрема, у ЗУ «Про виконання рішень та застосування практики Європейського суду з прав людини», Законі Великої Британії «Про права людини» та ін. З одного боку, у ЄКПЛ не має окремого розділу, який присвячено питанням ІТ-права, проте, її окремі норми мають прямий вплив на сферу інформаційних технологій.

Умовно можна виокремити чотири основні сфери впливу ЄКПЛ та рішень ЄСПЧ на ІТ-право: 1) право на приватність в цифрову епоху; 2) свобода вираження поглядів в інтернеті; 3) авторське право та суміжні права в цифровому середовищі; 4) доступ до інформації.

Хоча рішення ЄСПЛ можуть напряму не стосуватися ІТ-права, значна їх кількість мала ґрунтовний вплив на законодавство та галузь інформаційних технологій.

В даній статті розглядаються деякі з рішень ЄСПЛ.

Таблиця. 1. Окремі рішення ЄСПЛ, які вплинули на ІТ-право
[Individual decisions of the ECHR that have influenced IT law].

Справа	**Рік**	**Опис**	**Значення для ІТ-права**
S. and Marper v. the United Kingdom	2008	Зберігання біометричних даних.	Встановлення строків зберігання інформації, отриманої шляхом застосування інформаційних технологій.
Kopp v. Switzerland	1998	Прослуховування телефонних розмов.	Вплив на спостереження за даними в Інтернеті, контроль за зберіганням даних, регламентація перехоплення даних, захист конфіденційної інформації, правила транскордонної передачі даних.
Roman Zakharov v. Russia	2015	Моніторинг електронної комунікації.	Захист права на приватність в контексті моніторингу електронної комунікації роботодавцями.
Ahmet Yildirim v. Turkey	2012	Блокування доступу до сайту.	Встановлення умови пропорційності блокування інформації, захист посередницьких платформ, визнання Інтернету ключовою платформою для обміну інформацією та вираження поглядів.
Delfi AS v. Estonia	2015	Відповідальність провайдерів за коментарі користувачів.	Визначення відповідальності провайдерів за контент, який розміщують користувачі, необхідність модерації контенту з ознаками дифамації.
Ukraine v. Russia (re Crimea)	2024	Порушення свободи слова та доступу до інформації в Криму.	Підкреслення важливості дотримання свободи слова та доступу до інформації в онлайн-просторі.

Право на приватність в цифрову епоху ґрунтується на положенні, що кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції [2, ст.

8]. Дане положення має ключове значення для ІТ-права, адже впливає на питання збору, обробки та поширення інформації, узгодження меж приватного життя та національної безпеки, а також сферу державного нагляду та контролю. Як слушно зазначають О. В. Петришин та О. С. Гиляка, цифровізація практично усіх сфер життя призводить в деяких випадках і до негативного впливу, перш за все щодо забезпечення природних, невідчужуваних прав людини, особливо коли мова йде про недоторканність особистого життя [3, с. 30].

Право на приватність пов'язано зі збором та поширенням інформації, адже саме на цьому етапі відбувається втручання у приватне життя фізичної особи, яке визнається фундаментальним правом людини на міжнародному та конституційному рівнях. Даний процес уточняється додатковими нормативними актами, зокрема, Конвенцією 108 Ради Європи, в якій захист даних розглядається як захист основних прав і свобод людини [4]. На сьогодні вже понад сто двадцять країн світу в тому чи іншому обсязі ратифікували норми міжнародного законодавства про конфіденційність та захист персональних даних фізичних осіб, зробивши їх частиною національного законодавства, задля забезпечення суворішого захисту та здійснення пильного контролю у цій сфері [5, с. 28]. Наявність спеціальних правових норм зумовлює ІТ компанії впроваджувати у свої додатки та сайти спеціальні алгоритми для отримання згоди користувача на збір, обробку та використання інформації. В цьому контексті можна виділити дві показові судові справи, S. and Marper v. the United Kingdom (2008) та Kopp v. Switzerland (1998).

Справа S. and Marper v. the United Kingdom (2008) стосувалась збереження біометричних даних отриманих під час арешту двох осіб. ЄСПЛ постановив, що безстрокове зберігання даних фізичних осіб порушує принцип пропорційності та є втручанням у приватне життя [6]. Центральним питанням даної справи був не сам факт збирання інформації, а обов'язкове визначення строків її зберігання. Як наголошує О. М. Туазон, такі дані є конфіденційними, а їх зберігання може призвести до стигматизації та неналежного використання, що породжує необхідність дотримання балансу між спільним інтересом та правом на приватне життя [7]. Хоче це рішення стосується діяльності правоохоронних органів, воно мало значний вплив на законодавство різних країн та встановлення строків зберігання інформації, зокрема, отриманої шляхом застосування інформаційних технологій.

Справа Kopp v. Switzerland (1998) стосувалась втручання у приватне життя шляхом прослуховування телефонних розмов, які Г. С. Копп вчиняв відносно працівників своєї юридичної компанії, через підозру, що його дружина передає конфіденційну інформацію прокурору [8]. Суд звернув увагу на відсутність детального нормативного розмежування між професійною та приватною інформацією, а також відсутності належної регламентації порядку незалежного нагляду та наголосив, що професійна діяльність також підпадає від дію ст. 8 ЄКПЛ [9]. Дана справа мала важливий вплив на ІТ-право в декількох напрямках: 1) спостереження за даними в Інтернеті (зокрема, електронною поштою); 2) суворий контроль за зберіганням даних постачальниками телекомунікаційних послуг; 3) чітка регламентація порядку перехоплення даних урядовими інституціями; 4) захист конфіденційної інформації професійного характеру; 5) правила транскордонної передачі даних, зокрема, при співпраці правоохоронних органів.

Моніторинг електронної комунікації створює загрозу для дотримання права на приватність та потребує чіткої правої регламентації, адже може проводитись не лише державними установами, а й роботодавцями, які аналізують електронну пошту, історію пошукових запитів, тощо, своїх працівників. Показовою тут є справа Roman Zakharov v. Russia (2015) в якій суд підтримав позицію журналіста, який вимагав визнання національного законодавства своєї країни таким, що протирічить ст. 8 ЄКПЛ через дозвіл таємного перехоплення комунікації без судового контролю та чітких критеріїв для його санкціонування [10].

Порушення права на приватність розглядались і в інших справах ЄСПЛ, і хоча не всі вони на пряму пов'язані з ІТ сферою, вони мають прямий вплив на впровадження нових алгоритмів та правил збору, зберігання та поширення інформації.

Окремою проблематикою, якій ЄСПЛ приділяє значну увагу, є випадки приниження честі, гідності та ділової репутації (дифамації) в Інтернеті, а також доступ до Інтернету, обмеження якого може порушувати право на інформацію і протирічити ст. 10 ЄКПЛ, в якій йдеться про свободу вираження поглядів. Ш. Чхетри слушно наголошує, що метою законів про дифамацію є створення балансу між захистом індивідуальної репутації та свободою вираження поглядів, але на практиці, такі закони часто використовуються як засіб пригнічення [11, с. 1981]. У справі Ahmet Yildirim v. Turkey (2012) йшлося про блокування доступу до сай-

ту турецького науковця через загальне блокування всіх сайтів, створених на платформі Google Sites, а не через порушення, які вчинив позивач. Підставою для цього стало розміщення на іншому сайті інформації, яка принижує честь та гідність М. К. Ататюрка.

Застосування загального, а не індивідуального (вибіркового) підходу стало причиною визнання порушення ст. 10 ЄКПЛ. Суд визнав такі дії не пропорційними (блокування всього порталу слід застосовувати лише за крайніх обставин) та наголосив на необхідності ефективного судового перегляду актів про блокування веб-ресурсів, а також доцільності застосування вузько направлених санкцій з видалення контенту, а не блокування сайту, або платформи [12]. Держава має блокувати лише окремий контент, адже блокування всього ресурсу, на якому він був розміщений, призводить до порушення права на свободу вираження поглядів та доступу до інформації. За аналогією можна говорити про недоцільність блокування платформи YouTube або Facebook через окремі коментарі, або поширення інформації, яка визнана державою «небажаною». Дана справа є важливою для ІТ-права, адже встановлює умову пропорційності блокування інформації, захисту посередницьких платформ та визначення Інтернету ключовою платформою для обміну інформацією та вираження поглядів.

В контексті зазначеного, актуальною є дискусійна ситуація в Україні, пов'язана з критикою та обговоренням того, що Верховна Рада України 14 січня 2025 року прийняла у другому читанні та в цілому проект Закону про внесення змін до деяких законів України щодо посилення деяких гарантій діяльності медіа, журналістів та громадян на доступ до інформації, реєстр. №11321 від 05.06.2024 року [13]. В цьому проекті пропонується закріпити, що суб'єкти у сфері онлайн-медіа звільняються від відповідальності за поширення недостовірної інформації, а також інформації, заборона поширення якої передбачена статтями 36, 42 та 119 вказаного закону, якщо така інформація була поширена користувачами у розділах для коментування чи розміщення користувацьких публікацій на вебсайті чи веб-сторінці такого медіа, за умови що суб'єкт у сфері онлайн-медіа обмежив доступ до такої інформації впродовж трьох робочих днів не тільки з моменту отримання відповідної скарги чи припису Національної ради, а й з моменту отримання ухвали про відкриття відповідного провадження судом [14, с. 3]. Публічна критика була стосувалась нових обов'язків ЗМІ щодо видалення окремих коментарів, але, як пояснив Інститут масової інформації, даний проект закону не створює нових зобов'язань для медіа щодо видалення коментарів читачів, але звільняє їх від відповідальності за умови своєчасної модерації коментарів читачів, що можуть ображати людей, мати характер наклепу чи самі по собі порушувати закон, щоб не отримати судовий позов чи повістку на допит до слідчого [15].

В контексті відповідальності провайдерів та посередників за контент, який розміщують користувачі доцільно розглянути справу Delfi AS v. Estonia (2015). Естонський суд визнав компанію Delfi AS винною та зобов'язав її виплатити компенсацію за розміщення на її порталі інформації про скасування будівництва дороги, що призвело до появи негативних, образливих коментарів в адресу компанії-підрядника. Національний суд підтримав позицію останнього, що веб-портал несе відповідальність за коментарі, які розміщені на його сайті. ЄСПЛ також підтримав цю позицію, та наголосив на наступному: 1) власник сайту вів комерційну діяльність та отримував прибуток за рахунок відвідувачів його порталу; 2) Delfi AS мав інструменти для модерації неприйнятних коментарів; 3) негативні коментарі в адресу підрядника завдавали шкоду його діловій репутації; 4) через сукупність цих фактів, притягнення компанії Delfi AS до відповідальності не порушую ст. 10 ЄКПЛ [16].

Дана справа мала важливий прецедентний характер, а з урахуванням її змісту можна констатувати, що в певних випадках, суб'єкти у сфері онлайн-медіа мають аналізувати та видаляти інформацію (включно з коментарями третіх осіб), які мають ознаки дифамації, а тому, зазначений проект закону №11321 не протирічить ст. 10 ЄКПЛ.

Рішення ЄСПЛ мають важливе значення для розбудови національного законодавства України в сфері захисту даних та всього ІТ-права. Зокрема, ст. 8 та ст. 10 ЄКПЛ були дотримані у ЗУ «Про захист персональних даних», Типовому порядку обробки персональних даних, Порядку здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних та Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації

[17]. Також в Україні ведеться активна діяльність щодо імплементації в законодавство положень Конвенції про захист осіб щодо автоматизованої обробки персональних даних та GDPR (Загальний регламент захисту даних). Окрім цього, ще у 2021 році було подано проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації.

Рішення ЄСПЛ вплинули на українське ІТ-законодавство в різних напрямках, особливо, щодо збору та захисту інформації, авторського права, справедливого суду, доступу до інформації, свободи вираження поглядів. Актуальним прикладом останнього є судова справа Ukraine v. Russia (re Crimea) (2024) в якій ЄСПЛ, серед іншого, визнав відповідача винним у порушенні ст. 10 ЄКПЛ за утиск українських ЗМІ (включаючи онлайн) та обмеження свободи зібрань [18].

Окрім зазначеного вище, рішення ЄСПЛ свідчать про те, що учать у демократичних процесах потребує забезпечення фундаментального права на доступ до інформації та Інтернету. Це підкреслює нагальну потребу в актуалізації українського ІТ-законодавства для його відповідності стандартам ЄСПЛ.

Також, у контексті сучасної кібербезпеки та моніторингу, ЄСПЛ розробив структуру, яка забезпечує належний захист конфіденційності, одночасно вирішуючи питання безпеки. Такий моніторинг має здійснюватися законно і громадяни повинні знати, що відбувається, на яких підставах та в яких межах. Україна продовжує вносити зміни у свою кіберполітику та політику моніторингу відповідно до цілей, визначених у рішеннях ЄСПЛ.

Окремою темою можна виділити проблеми цифрового авторського права та суміжних прав. Розвиток інформаційних технологій вимагає нових форм творчості та методів використання існуючих творів, тому особливу увагу слід приділяти захисту авторського права на міжнародному рівні. З рішень ЄСПЛ можна побачити, що інтереси автора мають бути узгоджені з інтересами громадськості, що вимагає захисту права на доступ до інформації та свободу думки. В цьому контексті актуальним питанням визнається відповідальність постачальників послуг Інтернету та власників інтернет порталів за порушення авторських прав їхніми користувачами. У справі Promusicae v. Telefónica de España S.A.U. (2012), суд наголосив на тому, що відповідальність провайдерів не є сторонньою, але, в той же час, вони зобов'язані вжити заходів для блокування доступу до контенту, який порушує правові норми [19]. Це рішення має вирішальне значення для регулювання авторського права в кіберпросторі, оскільки воно позначає поріг відповідальності провайдера, а також процес блокування доступу до контенту.

Інше не менш важливе питання стосується захисту авторських прав на комп'ютерне програмне забезпечення. ЄСПЛ у справі SAS Institute Inc. v. World Programming Ltd. (2012) визнав, що ідеї та концепції комп'ютерної програми не підпадають під дію авторського права, але вихідний код, алгоритми та їх організація захищають законом [20]. Це судове рішення важливе для ІТ-права, адже воно сприяє творчості та суперництву, дозволяючи програмістам розробляти нове програмне забезпечення на основі змінених ідей без необхідності безпосередньо копіювати вихідний код програм.

Крім того, окремі рішення ЄСПЛ стосуються захисту баз даних, права на використання творів для навчання та обмеження авторського права з метою суспільної користі. Всі наведені судові рішення мають велике значення для подальшого розвитку ІТ-права та встановлення правового порядку в цифровому просторі.

ЄСПЛ залишається дуже активним у вирішенні питань, які стосуються авторського права в цифровому світі, беручи до уваги розвиток технологій та нові способи створення творів. Цей аспект практики ЄСПЛ має ключове значення для розвитку ІТ-законодавства України, оскільки допомагає узгодити національне право з європейськими принципами, з метою забезпечення ефективного захисту авторських прав у цифровій економіці.

З урахуванням зазначеного слід визнати, що одним з найбільш актуальних викликів для українського ІТ-законодавства є його гармонізація з європейськими стандартами, що характеризується низкою викликів: 1) рішення ЄСПЛ, в яких Україна не є стороною спору зазнають неоднозначності у застосуванні [21]; 2) швидкий розвиток технологій потребує постійної актуалізації законодавства, з урахуванням нових нормативних актів ЄС (зокрема, у сфері ШІ); 3) проблеми послідовності та ефективності застосування прецедентів ЄСПЛ [22]; 4) необхідність критичної оцінки ефективності українського законодавства та посилення механізмів інкорпорації міжнародного права у національне законодавство [23, с. 15].

Таблиця. 2. Виклики для IT-права України [Challenges for Ukrainian IT law].

Виклик	**Шляхи вирішення**
Неоднозначність застосування рішень ЄСПЛ, в яких Україна не є стороною спору.	Аналіз та адаптація рішень з урахуванням національної специфіки, розробка методичних рекомендацій для судів.
Швидкий розвиток технологій.	Постійний моніторинг нових технологій та їх правового регулювання, своєчасне внесення змін до законодавства, співпраця з експертами в галузі IT.
Проблеми послідовності та ефективності застосування прецедентів ЄСПЛ.	Підготовка судових збірників з практикою застосування рішень ЄСПЛ, проведення навчальних семінарів для суддів, підвищення рівня правової обізнаності населення.
Необхідність критичної оцінки ефективності законодавства.	Проведення регулярних досліджень ефективності законодавства, залучення громадськості до обговорення законопроектів, створення механізмів зворотного зв'язку.

Висновки. Рішення ЄСПЛ мають значний вплив на розвиток IT-права та, зокрема, українського законодавства у цій сфері, що призводить до внесення змін до існуючих нормативних актів та сприяє формуванню правової культури, орієнтованої на права людини. Досягнення цих цілей вимагає від України подальшого розвитку IT-сектору з дотриманням рішень, уже прийнятих на рівні ЄСПЛ, згідно з якими від України вимагається створити середовище, сприятливе для інновацій, одночасно захищаючи права людини та верховенство права.

Україні необхідно працювати над існуючими викликами, посилюючи механізми реалізації та забезпечення адекватного діалогу між державою та учасниками IT-ринку. В майбутньому це має забезпечити Україні IT-середовище, яке є дружнім до прав людини, захищає свободи, сприяє розвитку технологій і розбудові держави.

При проведенні подальших досліджень слід зосередитись на оцінці ефективності законодавчих та адміністративних втручань і впливу рішень ЄСПЛ на певні аспекти IT-права, особливо на національну безпеку, приватні правовідносини та ШІ. Це допоможе покращити державну політку в сфері IT, і допоможе зрозуміти взаємозв'язок між правами людини та інформаційними технологіями в Україні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Відновлення та системний післявоєнний розвиток України – переможниці в умовах нового світового правопорядку: аналіз, погляди, передбачення: міжнародна колективна монографія (Батанов О.В. та ін.) / за заг. ред. Бисаги Ю.М., Бєлова Д.М., Пироги І.С., Берч В.В., Скрипнюка О.В., Дешко Л.М., Заборовського В.В. та Продан В.І. Братислава, Ужгород: РІК-У, 2023. 288 с.

2. European Convention on Human Rights, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 URL: https://www.echr.coe.int/documents/d/echr/convention_ENG.

3. Петришин О. В., Гиляка О. С. Права людини у цифрову епоху : виклики, загрози та перспективи. *Вісник Національної академії правових наук України.* 2021. Т. 28. № 1. С. 7-35. URL: https://doi.org/10.37635/jnalsu.28(1).2021.15-23.

4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS 108. URL: https://rm.coe.int/1680078b37 .

5. Khudolii T. I. Personal data in the system of personal non-property rights of individuals on the internet: a general description. *Actual problems of native jurisprudence*. 2021. Vol. 4, no. 4. P. 25–30. URL: https://doi.org/10.15421/392175.

6. S. and Marper v. the United Kingdom (2008). URL: https://hudoc.echr.coe.int/fre?i=001-90051

7. Tuazon O. M. Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime? Journal of law and the biosciences. 2021. Vol. 8, no. 1. URL: https://doi.org/10.1093/jlb/lsab022.

8. Kopp v. Switzerland (1998). URL: https://hudoc.echr.coe.int/eng?i=001-58144.

9. Introduction to Swiss Law / A. Thier et al. ; ed. by M. Thommen. Sui Generis Verlag, 2022. URL: https://doi.org/10.38107/026.

10. Roman Zakharov v. Russia (2015). URL: https://hudoc.echr.coe.int/fre?i=001-159324.

11. Chhetri S. The defamation in the internet age: cyber defamation. Int'l JL mgmt. & human. 2021. Vol. 1, no. 4. P. 1981–1994. URL: http://doi.one/10.1732/IJLMH.25957.

12. Ahmet Yildirim v. Turkey (2012). URL: https://hudoc.echr.coe.int/fre?i=001-115705.

13. Прес-служба Апарату Верховної Ради України. Верховна Рада України прийняла Закон щодо посилення деяких гарантій діяльності медіа, журналістів та громадян на доступ до інформації. *Офіційний портал Верховної Ради України*. URL: https://www.rada.gov.ua/news/razom/257651.html.

14. Пояснювальна записка до проекту Закону України «Про внесення змін до деяких законів України щодо посилення деяких гарантій діяльності медіа, журналістів та громадян на доступ до інформації». Апарат Верховної Ради України. 215д9/1-2024/121773 від 03.06.2024 р.

15. Зеленчук В. Законопроєкт № 11321 не створює нових зобов'язань для медіа щодо видалення коментарів. Інститут масової інформації. URL: https://imi.org.ua/monitorings/zakonoproyekt-11321-ne-stvoryuye-novyh-zobov-yazan-dlya-media-shhodo-vydalennya-komentariv-imi-i66053.

16. Delfi AS v. Estonia (2015). URL: https://hudoc.echr.coe.int/fre?i=001-155105.

17. Baker McKenzie. Key data privacy and cybersecurity laws | Ukraine. Global Data Privacy and Cybersecurity Handbook. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/emea/ukraine/topics/key-data-privacy-and-cybersecurity-laws.

18. Ukraine v. Russia (re Crimea) (2024). URL: https://hudoc.echr.coe.int/eng?i=002-14347.

19. Gnatovskyy M., Ioffe Y. Twenty years of the ECHR in Ukraine. Blog of the European Journal of International Law. URL: https://www.ejiltalk.org/twenty-years-of-the-echr-in-ukraine/.

20. Promusicae v. Telefónica de España S.A.U. (2012). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62006CJ0275.

21. SAS Institute Inc. v. World Programming Ltd. (2012). URL: https://curia.europa.eu/juris/liste.jsf?num=C-406/10.

22. Dospehova E. For what Ukrainians often judged with Ukraine in the ECHR. Center for Civil Liberties. URL: https://ccl.org.ua/en/positions/for-what-ukrainians-often-judged-with-ukraine-in-the-echr/.

23. Spytska L. Problems of enforcement of judgments of the European Court of Human Rights in Ukraine. Social Legal Studios. 2024. Vol. 7, no. 3. P. 9–16. URL: https://doi.org/10.32518/sals3.2024.09.

Стаття надійшла до редакції 22.04.2025
Стаття рекомендована до друку 24.05.2025

M. V. HURA
PhD in Law,
Senior Lecturer of the Department of Civil Law Disciplines,
E-mail: m.gura@karazin.ua , ORCID: https://orcid.org/0000-0002-7695-7672
V.N. Karazin Kharkiv National University
Kharkiv, 61022, Svobody square, 4

THE SIGNIFICANCE OF THE ECHR CASE LAW FOR IT LAW

ANNOTATION. *Introduction.* The swift progress of information technologies and the diffusion of the latter into all spheres of life compels an uninterrupted enhancement of the legal regulation of the sphere of IT.

Summary of the main results of the study. In Ukraine, this process is further complicated by the necessity of bringing the national legislation into compliance with European norms, particularly with the practice of the European Court of Human Rights (ECHR). The paper analyses the most important rulings of the ECHR on the different aspects of the IT law: right to privacy in the information age (S. and Marper v. The United Kingdom, Kopp v. Switzerland, Roman Zakharov v. Russia), freedom of expression in the net (Ahmet Yildirim v. Turkey, Delfi AS v. Estonia), right to receive information (Ukraine v. Russia (re Crimea)).

Conclusion. The author pointed out that the decisions of the ECHR have a reasonable influence on Ukrainian legislation regarding personal data protection, censorship, Internet free speech, and providers' liability for hosted content, and they also contribute to developing a human rights culture. The author emphasised problematising the significant sectoral challenges and modalities of their solution.

KEYWORDS: *European Court of Human Rights, ECHR, IT law, European Convention on Human Rights, right to privacy, freedom of expression, access to information, protection of personal data.*

REFERENCES

1. Restoration and systemic post-war development of Ukraine - the winner in the new world legal order: analysis, views, predictions: international collective monograph (Batanov O.V. et al.) / edited by Y.M. Bysaha, D.M. Belov, I.S. Piroga, V.V. Berch, O.V. Skrypniuk, L.M. Deshko, V.V. Zaborovsky and V.I. Prodan (2023). : RIK-U., 288 p. (in Ukrainian).

2. European Convention on Human Rights, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5 URL: https://www.echr.coe.int/documents/d/echr/convention_ENG.

3. Petryshyn O.V., Hilyaka O.S. (2021) Human rights in the digital age: challenges, threats and prospects. *Bulletin of the National Academy of Law Sciences of Ukraine*. T. 28. № 1. P. 7-35. URL:

https://doi.org/10.37635/jnalsu.28(1).2021. P.15-23. (in Ukrainian).

4. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS 108. URL: https://rm.coe.int/1680078b37.

5. Khudolii T.I. (2021) Personal data in the system of personal non-property rights of individuals on the internet: a general description. *Actual problems of native jurisprudence*. Vol. 4, no. 4. P. 25–30. URL: https://doi.org/10.15421/392175. (in Ukrainian).

6. S. and Marper v. the United Kingdom (2008). URL: https://hudoc.echr.coe.int/fre?i=001-90051.

7. Tuazon O.M. (2021). Universal forensic DNA databases: acceptable or illegal under the European Court of Human Rights regime? *Journal of law and the biosciences*. 2021. Vol. 8, no. 1. URL: https://doi.org/10.1093/jlb/lsab022.

8. Kopp v. Switzerland (1998). URL: https://hudoc.echr.coe.int/eng?i=001-58144.

9. Introduction to Swiss Law / A. Thier et al.; ed. by M. Thommen. Sui Generis Verlag, 2022. URL: https://doi.org/10.38107/026.

10. Roman Zakharov v. Russia (2015). URL: https://hudoc.echr.coe.int/fre?i=001-159324.

11. Chhetri S. (2021). The defamation in the internet age: cyber defamation. Int'l JL mgmt. & human. Vol. 1, no. 4. P. 1981–1994. URL: http://doi.one/10.1732/IJLMH.25957.

12. Ahmet Yildirim v. Turkey (2012). URL: https://hudoc.echr.coe.int/fre?i=001-115705.

13. Press service of the Verkhovna Rada of Ukraine. The Verkhovna Rada of Ukraine adopted a law to strengthen some guarantees for media, journalists and citizens to access information. Official portal of the Verkhovna Rada of Ukraine. URL: https://www.rada.gov.ua/news/razom/257651.html. (in Ukrainian).

14. Explanatory Note to the Draft Law of Ukraine "On Amendments to Certain Laws of Ukraine on Strengthening Certain Guarantees of Media, Journalists and Citizens' Access to Information". Secretariat of the Verkhovna Rada of Ukraine. 215д9/1-2024/121773 від 03.06.2024 р. (in Ukrainian).

15. Zelenchuk V. (2025). Draft Law No. 11321 does not create new obligations for the media to remove comments. Institute of Mass Information.URL: https://imi.org.ua/monitorings/zakonoproyekt-11321-ne-stvoryuye-novyh-zobov-yazan-dlya-media-shhodo-vydalennya-komentariv-imi-i66053. (in Ukrainian).

16. Delfi AS v. Estonia (2015). URL: https://hudoc.echr.coe.int/fre?i=001-155105.

17. Baker McKenzie. Key data privacy and cybersecurity laws | Ukraine. Global Data Privacy and Cybersecurity Handbook. URL: https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook/emea/ukraine/topics/key-data-privacy-and-cybersecurity-laws.

18. Ukraine v. Russia (re Crimea) (2024). URL: https://hudoc.echr.coe.int/eng?i=002-14347.

19. Gnatovskyy M., Ioffe Y. (2017). Twenty years of the ECHR in Ukraine. Blog of the European Journal of International Law. URL: https://www.ejiltalk.org/twenty-years-of-the-echr-in-ukraine/.

20. Promusicae v. Telefónica de España S.A.U. (2012). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62006CJ0275.

21. SAS Institute Inc. v. World Programming Ltd. (2012). URL: https://curia.europa.eu/juris/liste.jsf?num=C-406/10.

22. Dospehova E. (2016). For what Ukrainians often judged with Ukraine in the ECHR. Center for Civil Liberties. URL: https://ccl.org.ua/en/positions/for-what-ukrainians-often-judged-with-ukraine-in-the-echr/.

23. Spytska L. Problems of enforcement of judgments of the European Court of Human Rights in Ukraine. *Social Legal Studios*. 2024. Vol. 7, no. 3. P. 9–16. URL: https://doi.org/10.32518/sals3.2024.09.

The article was received by the editors 22.04.2025
The article is recommended for printing 24.05.2025