Перкун Юлія Олександрівна,

здобувачки першого (бакалаврського) рівня вищої освіти
Факультету права та міжнародних відносин Київського столичного університету імені Бориса Грінченка

ВИКЛИКИ ЗАБЕЗПЕЧЕННЯ ПРАВ ЛЮДИНИ В ЕПОХУ ЦИФРОВИХ ТЕХНОЛОГІЙ: ПІДХОДИ ЄВРОПЕЙСЬКОГО СУДУ З ПРАВ ЛЮДИНИ

Актуальність теми. Упродовж останніх десятиліть людство здійснило значні кроки у вдосконаленні багатьох сфер життя. Проте саме XXI століття стало ерою стрімких технологічних інновацій. Сьогодні важко уявити повсякденність без соціальних мереж, інтернету та цифрових платформ, які об'єднують мільйони людей по всьому світу. Наші звички та спосіб життя суттєво змінилися: ми починаємо ранок з перегляду новин у смартфоні, слухаємо подкасти в дорозі, обмінюємося думками в соціальних мережах і маємо миттєвий доступ до необмежених обсягів інформації.

Цей цифровий прорив відкрив нові можливості для реалізації прав і свобод, однак він також спричинив появу нових загроз для фундаментальних прав людини. В епоху цифрових технологій суттєвої трансформації зазнає ціла низка фундаментальних прав людини. Право на приватність потерпає від масового збирання персональних даних і біометричного стеження; свобода вираження поглядів обмежується через проблеми модерації контенту та регулювання онлайн-платформ; право на недискримінацію опиняється під загрозою через алгоритмічну упередженість і цифрову нерівність; доступ до інформації ускладнюється поширенням дезінформації та маніпулятивного контенту; а право на справедливий суд трансформується під впливом автоматизованих систем правосуддя та новітніх викликів цифрового доказування. Ці комплексні виклики вимагають від Європейського суду з прав людини розробки нових підходів до інтерпретації усталених правових норм у контексті технологічних інновацій.

Порушення права на приватність, незаконне поширення персональних даних або зображень, мова ворожнечі онлайн, кіберпереслідування – ці явища дедалі частіше стають предметом розгляду не лише в національних юрисдикціях, а й у практиці Європейського суду з прав людини. У відповідь на ці виклики ЄСПЛ адаптує правозастосування до нових умов, намагаючись зберегти баланс між свободою вираження поглядів та захистом гідності, приватного життя й безпеки особи [1, с. 34].

Виклад основного матеріалу. Права людини не є сталою категорією - їхній зміст постійно розширюється у відповідь на соціальні трансформації, науковий прогрес і технологічні зміни. Європейський суд з прав людини, тлумачачи положення Конвенції про захист прав людини і основоположних свобод, підкреслює її динамічний характер, називаючи Конвенцію «живим інструментом», що повинен адаптуватися до нових викликів часу. Це означає не лише гнучкість у застосуванні правових норм, а й новий підхід до самого розуміння прав людини в контексті цифрового суспільства. Так, право на повагу до приватного життя, закріплене у статті 8 Конвенції, ЄСПЛ послідовно поширив на новітні форми комунікації: електронну пошту, мобільний зв'язок, онлайн-платформи, яких не існувало на момент її ухвалення [3. С. 5-6].

Цей підхід до осучаснення стандартів знайшов відображення й у праві Європейського Союзу: у преамбулі Хартії ЄС про основні права (2000 р.) наголошено, що захист прав людини повинен посилюватися з урахуванням суспільних змін, соціального прогресу та технологічного розвитку, аби зробити ці права більш чіткими та дієвими [2, с. 391].

На практиці здатність Конвенції реагувати на виклики цифрової доби яскраво ілюструє справа Big Brother Watch and Others v. the United Kingdom, що стосувалася масового спостереження у Великій Британії. Спецслужби використовували технології для перехоплення комунікацій, збору даних від провайдерів та обміну інформацією з іноземними партнерами. Група журналістів і НУО поставила під сумнів відповідність таких програм закону RIPA 2000 року, вказуючи на ризики для приватності та свободи вираження поглядів [4]. Суд, проаналізувавши аргументацію сторін, дійшов висновку про наявність порушення статті 8 Конвенції через недостатність процедурних гарантій та ефективного нагляду за реалізацією програми.

Критичний аналіз британської системи масового спостереження дозволив Європейському суду з прав людини виявити три фундаментальні недоліки, що порушують стандарти захисту прав людини. По-перше, процедура перехоплення даних не передбачала санкціонування незалежним від виконавчої влади органом, що ставило під сумнів її об'єктивність і законність. По-друге, у запитах на санкцію були відсутні чіткі категорії пошукових термінів, що створювало ризик надмірного втручання у приватне життя. По-третє, не було належного санкціонування використання ідентифікаторів конкретних осіб, що могло призвести до необґрунтованого стеження. Суд дійшов висновку, що такі недоліки суперечать вимогам «якості закону» та не відповідають принципам необхідності й пропорційності, які лежать в основі демократичного суспільства [5, С. 585-586].

На нашу думку, це рішення має визначальне значення не лише для правової системи Великої Британії, але й, ширше кажучи, для майбутнього розвитку масових програм спостереження та механізмів обміну розвідувальною інформацією в Європі загалом. Показово, що Суд не обмежився суто правовими критеріями, аналізуючи цифрові виклики, він також торкнувся глибших питань демократичного контролю та прозорості. В умовах стрімкого технологічного прогресу, коли держави отримують безпрецедентні інструменти для збору й аналізу персональних даних, постає нагальна потреба в переосмисленні стандартів захисту прав людини. Отже, рішення Великої палати ЄСПЛ підкреслює не лише актуальність, а й невідкладність розробки ефективних процедурних гарантій, які б адекватно відповідали вимогам цифрової епохи, залишаючись водночас у руслі цінностей Конвенції.

Додатково, з точки зору перспективи Дьюї щодо демократії, можна стверджувати, що відповідальність за процеси збирання даних, обробки машинного навчання та роботу платформ соціальних медіа повинна фокусуватися не лише на прозорості самих алгоритмів, але й, що важливо, на прозорості щодо того, хто конкретно включений у процес обробки даних, а хто, в свою чергу, виключений. Такий підхід до відповідальності, зокрема, за вхідні дані та їх подальшу обробку, є, без сумніву, надзвичайно важливим для підтримки демократичної участі в сучасному суспільстві. Адже тільки за умови забезпечення чіткої та справедливої участі усіх сторін у цьому процесі можна досягти більш інклюзивного та рівного підходу до соціальних даних [12, С. 77-78].

Важливим кроком у напрямі боротьби з цифровими загрозами стала Конвенція Ради Європи про кіберзлочинність 2001 року, також відома як Будапештська конвенція - перший міжнародний документ, спрямований на криміналізацію правопорушень у кіберпросторі, покращення механізмів розслідування таких злочинів і посилення міжнародної співпраці в цій сфері. Конвенція охоплює широке коло діянь - від незаконного доступу до комп’ютерних систем до розповсюдження шкідливих програм і порушення конфіденційності даних [10].

Проте особливо гострою залишається проблема онлайн-харасменту, що демонструє справа Volodina v. Russia (no. 2) від 14 вересня 2021 року. Її фабула стосувалася жінки, яка зазнала систематичного кіберпереслідування з боку колишнього партнера. Заявниця стверджувала, що він незаконно використовував її особисті дані та інтимні фотографії для створення фейкових акаунтів у соціальних мережах, відстежував її місцезнаходження через GPS-трекер, встановлений у сумці, а також надсилав погрози вбивством. Попри серйозність цих порушень, національні правоохоронні органи не забезпечили

належного розслідування, що й стало підставою для звернення до Європейського суду з прав людини [6].

Суд констатував порушення статті 8 Конвенції, підкресливши, що державні органи не виконали своїх позитивних зобов'язань щодо захисту приватного життя заявниці. Рішення стало важливим орієнтиром для розуміння кіберпереслідування як форми насильства, що вимагає активного реагування держави. ЄСПЛ акцентував, що наявність законодавчих норм є недостатньою без їх ефективного застосування на практиці. Влада має не лише забезпечити юридичну можливість реагування, а й реально вживати заходів для запобігання цифровим формам насильства. Це рішення формує чіткий стандарт: бездіяльність держави в умовах сучасних загроз у цифровому просторі може розцінюватися як порушення фундаментальних прав людини. Це рішення ЄСПЛ є надзвичайно актуальним і для української правозастосовної практики, оскільки демонструє необхідність ефективного реагування на цифрові загрози та насильство в умовах зростаючої ролі соцмереж. З огляду на це, стає очевидною потреба у не лише нормативному оновленні міжнародних інструментів, таких як Конвенція про кіберзлочинність, але й у практичному впровадженні стандартів ЄСПЛ через підготовку спеціалізованих правоохоронних структур, що розуміють особливості кіберпростору та вміють діяти швидко й ефективно на захист жертв цифрового насильства [10, с.13].

Водночас справа яскраво демонструє ключову проблему, пов’язану з Конвенцією Ради Європи про кіберзлочинність. Попри її важливість, документ не дає чітких інструкцій і рекомендацій для країн-учасниць щодо забезпечення ефективного правового реагування на такі злочини. Конвенція потребує суттєвого доповнення, яке включало б розробку більш конкретних механізмів захисту, а також інтерпретацію існуючих норм з урахуванням сучасних викликів цифрового середовища [10].

Аналізуючи проблематику захисту права на приватність у цифрову епоху, необхідно звернути особливу увагу на фундаментальні підходи Європейського суду з прав людини до балансування конкуруючих інтересів між правом на приватність (ст. 8 Конвенції) та свободою вираження поглядів (ст. 10 Конвенції). Яскравою ілюстрацією такого балансування стала знакова справа Von Hannover v. Germany (No. 2), де заявники, принцеса Кароліна фон Ганновер та її чоловік принц Ернст Август, оскаржували публікацію їхніх фотографій, зроблених без згоди під час відпочинку в Сен-Моріц (Швейцарія) та супроводжуваних статтями про хворобу князя Реньє, батька принцеси. Федеральний конституційний суд Німеччини, застосовуючи критерії з попереднього рішення ЄСПЛ у Von Hannover v. Germany (2004), частково

задовольнив вимоги заявників, заборонивши публікацію лише двох фотографій, тоді як щодо інших було визнано їхню інформаційну цінність та внесок у суспільно значущу дискусію. Це дозволило ЄСПЛ сформулювати концептуальні підходи до визначення меж між двома основоположними правами та встановити важливий прецедент для аналогічних справ [7; 9].

У подальшому рішенні Суд конкретизував п’ять ключових критеріїв, які слід враховувати при балансуванні між свободою слова та правом на приватність. Насамперед, інформація має нести суспільну цінність - лише тоді її публікація є виправданою, адже просте задоволення цікавості не є легітимною підставою для втручання. Другим критерієм є публічний статус особи: чим активніше вона бере участь у громадському житті, тим вужчими є межі її приватності, хоча повністю це право не втрачається. Третій критерій - попередня публічна поведінка: відкритість у минулому не означає автоматичну згоду на подальше розкриття особистої інформації. Четвертий аспект - контекст і форма поширення: має значення, як саме інформація була подана, з яким обсягом розголосу та якими можуть бути її наслідки для репутації особи. Нарешті, важливим чинником є спосіб здобуття контенту - приховане чи неетичне отримання інформації само по собі може становити порушення приватного життя, незалежно від її подальшого змісту [8].

Усі ці критерії набувають ще більшої ваги в умовах цифровізації та стрімкого обміну даними, що актуалізує необхідність поєднання стандартів ЄСПЛ із положеннями Загального регламенту про захист даних (GDPR). Регламент чітко окреслює принципи обробки персональних даних — законність, прозорість, обмеження мети, мінімізацію даних та відповідальність, – що дозволяє ефективно адаптувати європейські підходи до захисту приватності у цифровому середовищі. Таким чином, практика ЄСПЛ у поєднанні з механізмами GDPR створює цілісну систему захисту прав людини в інформаційну епоху [15].

Висновки. Підсумовуючи аналіз, можна стверджувати, що останні роки позначилися суттєвим прогресом у діяльності Європейського суду з прав людини в контексті захисту прав людини в цифрову епоху. Практика ЄСПЛ підтверджує, що Конвенція про захист прав людини та основоположних свобод є живим інструментом, здатним адаптуватися до реалій цифрового суспільства. У рішеннях, таких як Big Brother Watch and Others v. the United Kingdom чи Von Hannover v. Germany (No. 2), Суд не лише реагує на нові технологічні виклики, а й формує єдині стандарти правового захисту у сфері цифрових прав, зокрема щодо приватності, свободи вираження поглядів та захисту персональних даних. Ці стандарти набувають загальноєвропейського

значення, створюючи орієнтир для держав-учасниць Конвенції та забезпечуючи уніфікацію підходів у правозастосовчій практиці.

Однак самих судових рішень недостатньо. Сучасне правове середовище потребує не лише гнучкого тлумачення чинних норм, а й глибоких трансформацій на рівні національного законодавства. Держави мають кодифікувати цифрові права як окрему категорію прав людини, адаптувати судову процедуру до викликів цифрового середовища, забезпечити прозорість алгоритмічних процесів, оновити законодавство у сфері персональних і біометричних даних, а також створити ефективні механізми захисту від цифрового насильства та зловживань. У цьому контексті слід звернути увагу й на положення Конвенції про кіберзлочинність 2001 року (Будапештської конвенції), яка встановлює міжнародні стандарти боротьби з кіберзлочинами та регламентує порядок збирання електронних доказів, що має важливе значення для формування цифрової правової політики.

Цифровізація суспільства також стимулює переосмислення традиційного розподілу галузей права, оскільки інформаційні технології дедалі більше формують єдину логіку правового регулювання. У цьому контексті активно розвивається концепція цифрових прав як оновленої системи базових прав людини, реалізація яких здійснюється через інтернет та цифрове середовище. Попри відсутність усталеної класифікації, вже зараз виокремлюються ключові цифрові права: право на захист персональних і біометричних даних, цифрову освіту, свободу вираження поглядів та участь у цифровому обігу, а також право бути забутим. У фокусі обговорень залишається й визнання доступу до інтернету як самостійного суб’єктивного права людини [13, С. 22-24].

Водночас необхідно пам’ятати про дуалістичну природу цифрових технологій: з одного боку, вони посилюють реалізацію прав, а з іншого – створюють нові загрози. Алгоритмічна обробка цифрових слідів, метаданих і пошукових запитів здатна не лише формувати інформаційні бульбашки, а й розкривати приватні аспекти життя користувача, що зумовлює нагальну потребу в ефективних інструментах контролю за обробкою даних та захисту приватності в цифровому просторі [14, с. 8].

У цьому контексті особливе значення набуває Загальний регламент про захист даних (GDPR), який слугує зразком нормативного врегулювання цифрових прав у Європейському Союзі. Регламент встановлює високі стандарти обробки персональних даних, підзвітності, прозорості, згоди та права на забуття, що вже впливають на формування практики ЄСПЛ і можуть стати орієнтиром для держав, які прагнуть модернізувати свої національні правові системи.

Отже, повноцінне осмислення природи цифрових прав та їх місця в системі прав людини, а також належне нормативне закріплення та забезпечення механізмів реалізації є одним із найважливіших завдань для національних і міжнародних правових систем. Цей процес має бути не лише юридично вивіреним, а й етично чутливим до змін соціальних реалій та технологічного прогресу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Панкратова В. О., Шеін Д. С. Права людини в епоху інформаційних технологій. Право і безпека. 2021. № 3. С. 34.
2. Charter of Fundamental Rights of the European Union. Official Journal of the European Union. 2012/C 326/02. P. 391–407. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012P/TXT.
3. Гончаренко С.В. Права людини інформаційної доби. Вісник Академії адвокатури України. 2005. No 3(17). С. 5–6. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=vaau_2006_5_3.
4. CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM, Applications Nos. 58170/13, 62322/14 and 24960/15, Strasbourg, 25 May 2021. URL: https://hudoc.echr.coe.int/fre#{"itemid":["001-210077"]}.
5. American Journal of International Law , Volume 116 , Issue 3 , July 2022 , pp. 585 – 592, pp. 585-586. DOI: https://doi.org/10.1017/ajil.2022.35.
6. Volodina v. Russia (no. 2), no. 40419/19, Judgment of 14 September 2021, European Court of Human Rights. URL: https://hudoc.echr.coe.int/eng-press?i=003-7116031-9638379 Date of access: 04.05.2025.
7. CASE OF VON HANNOVER v. GERMANY (No. 2), Applications Nos. 40660/08 and 60641/08, Judgment of 7 February 2012. – Strasbourg: European Court of Human Rights. – URL: https://hudoc.echr.coe.int/fre#{"itemid":["001-109029"]}.
8. Von Hannover v. Germany (No. 2) // Global Freedom of Expression. Columbia University. 2012. URL: https://globalfreedomofexpression.columbia.edu/cases/von-hannover-v-germany-no-2/.
9. Case Of Von Hannover v. Germany. URL: https://hudoc.echr.coe.int/eng?i=001-61853.
10. Конвенція про кіберзлочинність, 2001: Конвенція Ради Європи. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
11. Commissioner for Human Rights. (2012). Social Media and Human Rights: Issue Discussion Paper (CommDH (2012)8). Strasbourg. P. 22 – p.13 URL: https://rm.coe.int/16806da579.
12. Jørgensen, R. F. (Ed.). Human Rights in the Age of Platforms. Cambridge: The MIT Press, 2019. 343 p.
13. 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. С. 22-24.
14. Galindo, F., & Garcia-Marco, J. (2017). Freedom and the Internet: Empowering citizens and addressing the transparency gap in search engines. European Journal of Law and Technology, 8(2), PP. 1-18. P. 8.
15. 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, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://gdpr-info.eu.