

ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА; ІСТОРІЯ ПОЛІТИЧНИХ І ПРАВОВИХ УЧЕНЬ

УДК 004.056.55:340.13:17.023.34

DOI <https://doi.org/10.32782/TNU-2707-0581/2025.1/01>

Горелова В.Ю.

Таврійський національний університет імені В.І. Вернадського

ЦИФРОВІ ПРАВА: ЕТИЧНІ АСПЕКТИ ТА ВИКЛИКИ

Стаття присвячена аналізу етичних і правових аспектів захисту прав людини в умовах глобальної цифровізації. У статті наголошено увагу на актуальності теми, зумовленій швидким розвитком інформаційних технологій, що створює нові можливості, але водночас і загрози для приватності, свободи слова та рівного доступу до цифрових ресурсів.

Основними проблемами, розглянутими у статті, є порушення конфіденційності, цифрова нерівність, алгоритмічна упередженість та домінування великих технологічних компаній (Big Tech). Зокрема, аналізуються такі резонансні кейси, як скандал із Cambridge Analytica, програма PRISM та випадки цифрової дискримінації, пов'язані з алгоритмічними системами, така як гендерна упередженість в алгоритмах найму Amazon.

У статті підкреслено важливість розробки комплексного підходу до захисту цифрових прав, що включає посилення міжнародного регулювання, розвиток технологій для захисту персональних даних (VPN, шифрування), забезпечення прозорості алгоритмів та впровадження етичних стандартів. Особливу увагу приділено етичній відповідальності держав, корпорацій та громадянського суспільства у створенні безпечного та справедливого цифрового середовища.

Використано міждисциплінарний підхід, що поєднує правовий аналіз, етичні дослідження та метод кейс-стаді. Проведений аналіз міжнародних регламентів, наукових публікацій і практичних прикладів дозволив окреслити основні напрями удосконалення правового та технологічного регулювання в сфері цифрових прав.

Авторка робить висновок про необхідність гармонізації правових норм на глобальному рівні, створення міжнародних стандартів для регулювання діяльності технологічних корпорацій, а також активного розвитку технологічних рішень, що забезпечать захист даних і недопущення монополізації цифрового простору. Також у статті наголошується на важливості підвищення цифрової грамотності серед населення як одного з ключових факторів у захисті цифрових прав.

Матеріали і методи. У статті використано міждисциплінарний підхід, що поєднує правовий аналіз, етичні дослідження та кейс-метод. Основними методами аналізу були порівняльний правовий аналіз для вивчення законодавчих ініціатив у різних юрисдикціях, контент-аналіз для оцінки публікацій з етичних питань та метод кейс-стаді для дослідження конкретних прикладів порушення цифрових прав. Джерелами даних слугували наукові публікації, міжнародні регламенти, а також практичні приклади, що ілюструють проблеми цифрових прав. Аналіз включає огляд сучасного законодавства, етичних принципів.

Результати проведеного дослідження. У результаті дослідження визначено основні виклики та морально-етичні аспекти цифрових прав у контексті глобальної цифровізації. Аналіз виявив ключові проблеми серед яких порушення конфіденційності користувачів, цифрова нерівність, алгоритмічна упередженість та проблемні питання домінування великих технологічних компаній Big Tech у цифровому середовищі. Дослідження підкріплене аналізом конкретних кейсів таких як скандал із Cambridge Analytica програма масового стеження PRISM та випадки цифрової дискримінації.

Зазначена проблематика. Зазначена проблематика охоплює такі ключові аспекти: 1) порушення конфіденційності (масове збирання персональних даних без згоди користувачів як у випадку PRISM підриває основи права людини на приватність, приналежно, витоки даних такі як інцидент із Facebook у 2021 році демонструють вразливість навіть найбільших платформ); 2) цифрова нерівність (нерівний доступ до інтернету та технологій поглиблює соціально-економічний розрив зокрема в країнах що розвиваються де доступ до Інтернету обмежений); 3) алгоритмічна упередженість (використання штучного інтелекту без належної етичної оцінки призводить до дискримінаційних рішень як це сталося із системою найму Амазон що проявила гендерну упередженість); 4) проблемні питання впливу великих компаній (наприклад, корпорації Google та Facebook не лише контролюють ринок цифрових послуг але й мають значний вплив на політичні та соціальні процеси). Зазначене викликає питання про монополію, тобто про порушення антимонопольного законодавства та недостатню прозорість в обробці персональних даних. Для ефективного вирішення зазначених викликів необхідна міжнародна співпраця, розробка чітких правових норм і активне впровадження етичних стандартів у сфері цифрових технологій.

Перспективи. Перспективи розвитку цифрових прав полягають у створенні глобальної нормативної бази що забезпечуватиме справедливий і безпечний цифровий простір для всіх користувачів. Подальші дослідження мають бути спрямовані на розробку універсальних міжнародних стандартів, які регулюватимуть діяльність великих технологічних корпорацій, забезпечуючи прозорість алгоритмів, захист персональних даних та недопущення монополізації цифрових ринків.

Особливу увагу слід приділити розвитку технологічних рішень, які гарантуватимуть максимальний рівень приватності та безпеки у цифровому середовищі. Зокрема перспективними, є децентралізовані платформи шифрування кінцевих точок, та інструменти для незалежного аудиту алгоритмів. Ці інновації мають стати основою для забезпечення контролю користувачів над власною інформацією, та запобігання несанкціонованому доступу.

Слід зазначити, що не менш важливим напрямом, має стати аналіз етичних аспектів використання штучного інтелекту, зокрема в питаннях алгоритмічної упередженості та впливу на соціальні економічні й політичні процеси. Саме впровадження механізмів контролю за алгоритмами та забезпечення їхньої відповідності етичним нормам, стане важливим кроком до збереження справедливості в цифровому середовищі.

Ключові слова: правове регулювання, етичні стандарти, цифрова безпека, цифрові права.

Постановка проблеми. Цифровізація перетворилася на ключову складову сучасного життя, охоплюючи всі сфери суспільного буття. Швидкий розвиток технологій створює нові можливості для комунікації, доступу до знань і участі у глобальних процесах. Проте водночас виникає низка серйозних етичних та правових викликів, пов'язаних із захистом цифрових прав, конфіденційності та свобод людини в інформаційному просторі. Одним із ключових проявів важливості проблематики захисту цифрових прав стали випадки масових витоків даних і неетичного використання персональної інформації.

Найбільш показовим прикладом є ситуація з Cambridge Analytica, коли у 2018 році, стало відомо про неправомірний доступ до даних мільйонів користувачів Facebook [1]. Цей інцидент став одним із найгучніших викликів для компанії Meta що володіє платформою Facebook. Основна критика полягала у тому що Meta не забезпечила належного інформування користувачів про ризики пов'язані з використанням їхніх даних консалтинговою компанією Cambridge Analytica, яка брала

активну участь у президентських виборах Сполучених Штатах Америки в 2016 році, отримавши доступ до даних 87 мільйонів осіб без їхньої згоди. Зібрана інформація використовувалася для персоналізованої політичної реклами спрямованої на вплив на американський електорат. Цей скандал став поворотною точкою у сфері захисту конфіденційності даних і корпоративної відповідальності, викликавши низку урядових розслідувань судових позовів і слухань у Конгресі США.

Пізніше, у 2019 році Комісія з цінних паперів і бірж США, SEC вжила заходів проти Facebook, що призвело до врегулювання на суму 100 мільйонів доларів [2]. Цей випадок висвітлив серйозні етичні, юридичні та фінансові наслідки для корпорацій, що ігнорують питання захисту приватності користувачів. Резонанс справи Cambridge Analytica суттєво вплинув на зміну громадської думки посиливши вимоги до жорсткішого регулювання діяльності компаній що займаються збором і обробкою особистих даних. Це спричинило глобальну дискусію щодо етичної відповідальності технологічних компаній, та їхньої від-

повідності моральним і правовим нормам. Такі події підкреслюють наявність суттєвих прогалин у регулюванні цифрового середовища, де інтереси бізнесу часто переважають над правами людини.

У цьому контексті актуальність теми захисту цифрових прав, набуває особливої значущості, оскільки вона стосується фундаментальних прав людини у новій цифровій реальності, котра постійно розвивається. Тема цифрових прав нерозривно пов'язана із забезпеченням соціальної справедливості та рівності людини. У розвинених країнах доступ до цифрових технологій стає базовою потребою, тоді як у країнах, що розвиваються, це питання залишається проблематичним. Відсутність рівного доступу до технологій спричиняє ще більше розшарування суспільства, формуючи нові форми цифрового розриву. Тому важливо враховувати не лише технічні аспекти, але й етичні, спрямовані на забезпечення рівноправного доступу та захисту даних усіх користувачів.

Отже, актуальність теми цифрових прав, етики та моральних викликів, які виникають у процесі глобальної цифровізації, зумовлена необхідністю створення більш прозорого та етичного цифрового середовища. Без активного втручання суспільства, законодавчих ініціатив та технологічного прогресу ці питання ризикують залишитися без належного вирішення, що може мати критичні наслідки для розвитку сучасного світу.

Аналіз останніх досліджень і публікацій. Проблематика цифрових прав активно досліджується в наукових колах, зосереджуючи увагу на питаннях конфіденційності, алгоритмічної упередженості, впливу технологічних корпорацій та етичних стандартів у цифровому середовищі. У цьому контексті важливо зазначити роботи наступних дослідників: Брюс Шнайєр (Schneier, B. (2021), який у своїй роботі *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. W. W. [3], детально аналізує загрози пов'язані з масовою цифровізацією та вразливістю інформаційних систем підкреслюючи необхідність комплексного підходу до захисту персональних даних; К. Гіттон (Guitton, C. (2020)) в журналі *Journal of Digital Information* у статті *Digital Privacy and the Protection of Data* [4], розглядає питання цифрової приватності та виклики, пов'язані із захистом даних у глобальному інформаційному середовищі, акцентуючи увагу на потребі міжнародної гармонізації законодавства; Біннс, Р. (2022) у роботі «*Algorithmic Bias and Its Impact on Society*» [5] аналізує алгоритмічну упередженість як прояв цифрової дискримінації, що

виникає внаслідок використання штучного інтелекту без належного етичного контролю. Шошана Зубофф (Zuboff, S. (2019)) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power in Public Affairs* [6], досліджує концепцію «капіталізму спостереження», зосереджуючи увагу на впливі великих технологічних корпорацій на приватність та права користувачів у цифровому середовищі; 7) Л. Флоріді (Floridi, L. (2014)) *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* в *Oxford University Press* [7], аналізує зміни в етичних та соціальних структурах, спричинені цифровою трансформацією суспільства, акцентуючи увагу на необхідності адаптації правових стандартів до нових реалій; 8) Кейт Кроуфорд (Crawford, K. (2021)) *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence* в *Yale University Press* [8] досліджує етичні виклики, пов'язані з використанням штучного інтелекту, зокрема питання дискримінації та маніпуляцій алгоритмічними системами; 9) Лоуренс Лессіг (Lessig, L. (2006)) *Code: And Other Laws of Cyberspace, Version 2.0*. в *Basic Books* [9], розглядає питання правового регулювання Інтернету, підкреслюючи роль коду як інструменту контролю та його вплив на цифрові права користувачів; 10) Деніел Солове (Solove, D. J. (2008)) *The Digital Person: Technology and Privacy in the Information Age* в *NYU Press* [10], аналізує проблеми захисту конфіденційності в епоху цифрових технологій, приділяючи увагу юридичним і етичним аспектам обробки персональних даних; 11) Кеті О'Ніл (O'Neil, C. (2016)) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* в *Crown Publishing* [11], досліджує, як алгоритмічні системи можуть поглиблювати соціальну нерівність, створюючи нові форми дискримінації в цифровому середовищі; 12) Зейнеп Тюфекчі (Tufekci, Z. (2015)) *Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency* в *Colorado Technology Law Journal* [12], розглядає вплив алгоритмічних рішень на суспільство, включаючи питання контролю над інформаційними потоками та маніпуляції свідомістю користувачів.

Окрім того, Європейська Комісія (European Commission. (2022)) пропонує регламент *Artificial Intelligence Act: Proposal for a Regulation* [13], для регулювання використання штучного інтелекту, зосереджуючи увагу на прозорості алгоритмів і відповідальності компаній перед користувачами. Також слід зазначити документ ООН (United Nations. (2021)) *The Role of the United Nations in*

Digital Rights Protection [14], в якому визначено роль міжнародних організацій у формуванні політик захисту цифрових прав, включаючи механізми контролю над технологічними компаніями.

Постановка завдання. Метою статті є аналіз етичних і правових аспектів захисту прав людини в умовах глобальної цифровізації, що сприяє формуванню безпечного, прозорого та етичного цифрового середовища, яке забезпечить рівні права та можливості для всіх користувачів.

Результати дослідження спрямовані на підвищення обізнаності про цифрові права та розробку практичних рішень для їх захисту. Стаття є внеском у міжнародний дискурс щодо гармонізації правових, технологічних і етичних аспектів цифровізації.

Виклад основного матеріалу. Цифрові права являють собою нову категорію фундаментальних прав людини, адаптованих до реалій цифрової епохи. Суть цифрових прав, полягає у забезпеченні захисту основних свобод і прав індивіда у цифровому середовищі. Це включає доступ до інформації, свободу слова, конфіденційність та рівність можливостей у використанні технологій. У сучасному світі цифрові права стали невіддільною складовою прав людини, зважаючи на те, що дедалі більше аспектів соціального, економічного та політичного життя переміщується в онлайн-простір. Спроби визначити і впорядкувати ці права на глобальному рівні були зроблені у численних ініціативах. Однією з таких є «Конституція Інтернету», запропонована Тімоті Бернерсом-Лі [15]. «Конституція Інтернету» – концепція, що покликана визначити основні принципи, які повинні регулювати розвиток Інтернету. Охоплюючи такі фундаментальні права користувачів як свобода слова, право на приватність та доступ до інформації, ця ініціатива наголошує на важливості відкритості та нейтральності мережі, що забезпечує інновації і креативність у цифровому середовищі. Концепція спрямована на створення універсальної системи принципів, що гарантують доступність, безпеку та відкритість Інтернету для кожної людини. Дана концепція передбачає, що кожен користувач має право на вільний доступ до інформації, захист персональних даних та рівноправну участь у цифрових процесах. Етична основа цифрових прав базується на принципах рівності та справедливості, що вимагають забезпечення однакових можливостей для всіх користувачів незалежно від їхнього соціального статусу, місця проживання чи економічного стану. Водночас моральний аспект цифрових прав зосереджений

на відповідальності держав, корпорацій і суспільства за захист цих прав. Порушення конфіденційності, обмеження доступу до інформації чи контроль свободи слова у цифровому просторі є викликами, які підривають основи демократичних цінностей і створюють небезпечні прецеденти для майбутнього розвитку цифрової ери.

Цифрові права потребують чіткого нормативного закріплення та практичної реалізації, адже без належного регулювання вони залишаються лише декларативними. Глобальна ініціатива зі створення нормативної бази для цифрових прав, подібна до ініціативи Бернерса-Лі [15], має ключове значення для забезпечення стабільного та справедливого розвитку цифрового суспільства, де етичні та моральні принципи будуть основою регулювання взаємодії людини і технологій.

Наступним ключовим напрямом вирішення проблем у сфері цифрових прав, є посилення правового захисту. У зв'язку з глобальними викликами, що постають перед цифровим середовищем, зокрема в питаннях конфіденційності даних, монополії великих технологічних компаній, захисту прав користувачів, важливим кроком постає розробка та впровадження міжнародних стандартів, що регулюватимуть діяльність в цифровому просторі. Прикладом успішної моделі є Загальний регламент захисту даних (GDPR), прийнятий Європейським Союзом у 2018 році [16]. Цей регламент встановлює високі вимоги до обробки персональних даних і визначає чіткі правила для компаній, що працюють на європейському ринку, включаючи обов'язок надавати користувачам можливість контролювати свої дані та право на забуття. Загальний регламент захисту даних став моделлю для інших країн, які почали розробляти свої власні законодавчі акти, орієнтуючись на європейський підхід, і дозволив забезпечити більш високий рівень захисту персональних даних на міжнародному рівні.

Однією з найбільших проблем, що виникають у контексті цифрових прав, є відсутність ефективного та актуального законодавства для регулювання діяльності великих технологічних компаній, що мають значний вплив на глобальний цифровий ландшафт. Проблема регулювання Big Tech стає особливо актуальною у зв'язку з їхньою монополістичною діяльністю, впливом на економіку, політику та соціальні процеси. Великі технологічні компанії, такі як Google [17], Facebook [18], Amazon [19] та інші, володіють величезними ресурсами, які дозволяють їм домінувати на ринку і формувати громадську думку через плат-

форми, що охоплюють мільярди користувачів по всьому світу. Одним із найбільш яскравих прикладів порушень з боку таких компаній є регулярні юридичні розгляди, що проводяться проти Google та Facebook в Європейському Союзі. Вони стосуються звинувачень у порушенні антимонопольного законодавства, а також неповного або нена належного виконання вимог Загального регламенту захисту даних (GDPR) [16]. Оскільки ці компанії збирають та обробляють величезну кількість персональних даних, вони піддаються критиці за недостатній рівень захисту приватності своїх користувачів.

Проблеми з монополією також виявляються у тому, як ці компанії контролюють ринки цифрової реклами, що дозволяє їм зловживати своєю домінуючою позицією, обмежуючи конкуренцію. Законодавча недостатність у регулюванні діяльності великих технологічних компаній є результатом швидкого розвитку цифрових технологій, яке випереджає можливості національних урядів і міжнародних організацій адаптувати існуюче законодавство. Багато з нині діючих законів, зокрема в сфері захисту даних та антимонопольної політики, були розроблені до ери широко-масштабного використання інтернет-платформ і не враховують усі аспекти сучасної цифрової економіки. В результаті виникають прогалини в правовому регулюванні, які дозволяють великим технологічним компаніям обходити обмеження, створюючи монополії, порушуючи конфіденційність і не забезпечуючи належного захисту інтересів користувачів. Необхідність оновлення законодавства, вимагає створення нових міжнародних стандартів і законів, які зможуть ефективно регулювати діяльність Big Tech. Важливим аспектом є забезпечення рівних умов для всіх учасників цифрового ринку, захист прав користувачів і конкурентної боротьби, а також надання органам влади інструментів для контролю над діяльністю технологічних компаній. Ці виклики потребують не лише зміни національних підходів, але й міжнародної співпраці для створення комплексної правової бази, яка відповідатиме вимогам нової цифрової реальності.

Однією з найбільших проблем у сфері цифрових прав є порушення конфіденційності користувачів унаслідок широкомасштабного стеження за особою інформацією. Сучасні технології, які дозволяють збору, зберігання та аналізу величезних обсягів даних, відкривають нові горизонти в управлінні інформацією, але водночас створюють значні ризики для приватності. Порушення

конфіденційності є не лише питанням правового регулювання, але й етичним викликом для суспільства.

Найбільш резонансним випадком масового стеження стало викриття програми PRISM [20], коли колишній співробітник Агентства національної безпеки США [21] Едвард Сноуден розкрив масштабне спостереження за інтернет-комунікаціями громадян усього світу. Програма PRISM стала символом глобальних дискусій щодо конфіденційності законності та етики цифрового нагляду. Масовий збір даних без згоди користувачів порушує фундаментальні права людини піддаючи ризику правові принципи такі як четверта поправка до конституції США. Відсутність доказів причетності осіб до злочинів, ставить під сумнів моральні межі державного контролю. Використання персональних даних громадян без їхнього відома, суперечить міжнародним нормам і провокує дипломатичну напруженість. Таким чином, закритість роботи програми PRISM [20], створює простір для зловживань і підриває довіру до влади. Попри окремі спроби обмежити такі практики, проблема масового стеження залишається актуальною вимагаючи пошуку балансу між національною безпекою та правами людини.

Захист конфіденційності є фундаментальним аспектом цифрових прав оскільки особисті дані користувачів постійно збираються та обробляються глобальними компаніями важливо забезпечити ефективні механізми контролю над власною інформацією технологічні рішення такі як VPN сервіси та додатки для шифрування відіграють ключову роль у цьому процесі VPN дозволяють приховувати онлайн активність захищаючи користувачів від стеження рекламодавців та кіберзагроз тоді як зашифровані месенджери такі як signal унеможливають перехоплення приватних комунікацій ці технології не лише зміцнюють цифрову безпеку а й формують нові етичні стандарти взаємодії в цифровому просторі у поєднанні з ефективним правовим регулюванням вони сприяють створенню більш безпечного та справедливого цифрового середовища.

Ці проблеми акцентують увагу на необхідності розробки більш ефективних механізмів захисту конфіденційності в цифровому середовищі. Адже технології, що сприяють розвитку сучасних інформаційних систем, одночасно створюють ризики для безпеки особистих даних [22]. Важливо, щоб регулятори, технологічні компанії та громадськість знаходили спільне розуміння у створенні таких стандартів безпеки, які збері-

гають баланс між інтересами розвитку інтернет-технологій і правами користувачів на конфіденційність та захист від зловживань.

Інший важливий етичний аспект стосується проблеми цифрової нерівності, яка виявляється у нерівному доступі до Інтернету та сучасних технологій. У той час як розвинуті країни забезпечують своїм громадянам майже повну цифрову інтеграцію, значна частина населення світу все ще залишається відключеною від глобальної мережі.

Наприклад, згідно з даними Міжнародного союзу електрозв'язку (ITU), станом на 2019 рік лише 28,2% населення Африки мали доступ до Інтернету, що означає, що близько 71,8% були без підключення [23]. А за інформацією, опублікованою на порталі TechToday у листопаді 2024 року, в регіоні Африки на південь від Сахари близько 60% населення не користуються мобільним Інтернетом, незважаючи на наявність покриття [24]. Ці дані свідчать про значні бар'єри для доступу до Інтернету в Африці, що впливає на можливості населення в різних сферах життя. Це обмежує їхні можливості в освіті, працевлаштуванні та соціальній участі.

Така нерівність не лише поглиблює соціально-економічний розрив між країнами, а й ставить під загрозу реалізацію ідеї цифрових прав як універсального стандарту. Етична дилема полягає у пошуку способів мінімізувати ці проблеми, зберігаючи водночас фундаментальні свободи людини. Це вимагає узгодження інтересів різних зацікавлених сторін: держав, технологічних компаній і громадянського суспільства. Розвиток технологій має супроводжуватися впровадженням етичних стандартів, які б забезпечували прозорість, рівність та відповідальність у цифровому просторі [25].

Цифрова дискримінація стала важливою проблемою сучасного суспільства, що виникає внаслідок розширення використання алгоритмів та автоматизованих систем прийняття рішень. Одним із проявів цієї дискримінації є алгоритмічна упередженість, коли штучний інтелект або інші автоматизовані системи, через неправильно налаштовані параметри або історичні упередження, приймають рішення, що несправедливо ставлять у неприємне становище окремі соціальні групи. Яскравим прикладом такого упередження є система найму, яку розробила компанія Amazon [26] для автоматизації процесу відбору кандидатів. Алгоритм, розроблений для оцінки резюме, виявився упередженим щодо жінок, оскільки його навчали на історичних даних, де більшість

кандидатів на технічні посади були чоловіками. В результаті алгоритм віддавав перевагу кандидатам-чоловікам, що спричинило значну критику щодо гендерної дискримінації в алгоритмічному відборі [27]. Отже цифрова дискримінація проявляється не лише через алгоритмічну упередженість, а й через нерівний доступ до технологій та інтернету, що формує соціально-економічну нерівність у цифрову епоху. Саме мережевий доступ є ключовим фактором громадської політичної та економічної участі, проте уряди використовують інтернет-цензуру як засіб контролю, тим самим обмежуючи свободу слова і доступ до інформації. Яскравий приклад таких обмежень спостерігався в Ірані, де блокування інтернету під час протестів, позбавляло громадян можливості комунікації, організації протестів та отримання достовірних новин. Технології що мали б сприяти прозорості, натомість стають механізмом придушення свобод і поглиблення цифрового розриву між державою та суспільством [28].

Наведені аргументи дають змогу зробити висновок, стосовно значущості проблематики цифрових прав у контексті глобалізації, інформаційного простору, що визначається численними викликами, які постають перед суспільством, у процесі взаємодії людини та технологічних систем. Тобто, формування правового поля щодо захисту персональних даних, забезпечення цифрової безпеки, прозорості алгоритмів є необхідною умовою сталого розвитку цивілізації.

Слід зауважити, що глобалізація цифрового середовища висуває потребу в посиленні міжнародного співробітництва та стандартизації принципів захисту особистих даних. Серед таких ініціатив слід виокремити розвиток міжнародного права у сфері цифрових технологій та створення загальносвітових етичних норм, що базуються на принципах прозорості, доступності та справедливості. Прикладом успішної регуляторної моделі є впровадження GDPR, що дозволило суттєво підвищити рівень контролю за обробкою персональних даних та відповідальності компаній за їхнє використання [29].

Технологічний прогрес зумовлює необхідність розробки інноваційних методів забезпечення цифрової приватності. Одним з ефективних підходів є застосування технологій децентралізованого зберігання та шифрування даних, які гарантують користувачам контроль над їхньою інформацією. Саме використання протоколів шифрування кінцевих точок, у такому месенджері як Telegram, сприяє формуванню безпечного цифрового серед-

овища, мінімізуючи ризики несанкціонованого доступу.

Комплексний підхід до вирішення проблем цифрових прав, включає чотири основні компоненти, а саме: 1) посилення міжнародного регулювання; 2) розвиток технологій для захисту персональних даних; 3) забезпечення прозорості алгоритмів; 4) підвищення рівня цифрової грамотності серед населення. Важливою складовою цього підходу, є моральна відповідальність держав, технологічних компаній та громадян, які повинні активно сприяти створенню безпечного цифрового середовища. Держави мають забезпечувати ефективно законодавче регулювання діяльності технологічних корпорацій, впроваджувати політики що гарантують захист персональних даних громадян. Компанії зобов'язані впроваджувати етичні принципи в розробку та використання цифрових технологій, зокрема забезпечувати прозорість алгоритмів та їхню незалежну експертизу.

Також слід зазначити, що важливим напрямом є розвиток технологій таких як VPN, сервіси шифрування даних і децентралізовані системи. Ці технології надають користувачам більшого контролю над їхньою інформацією та повинні бути поєднанні з законодавчими ініціативами. Саме це сприятиме зменшенню кіберзагроз та несанкціонованого використання особистих даних [30].

Висновки. Розвиток цифрового середовища актуалізує потребу в комплексному підході до захисту прав людини. У віртуальному просторі, де поєднуються питання конфіденційності, свободи вираження поглядів, рівного доступу до технологій та впливу штучного інтелекту на соціальну взаємодію. Аналіз проблематики цифрових прав засвідчив, що головні виклики полягають у глобалізованому контролі над даними, домінуванні технологічних корпорацій, алгоритмічній упередженості та недостатньому рівні цифрової грамот-

ності населення. Особливу увагу слід приділити гармонізації правових норм на міжнародному рівні з урахуванням нових реалій інформаційного суспільства.

Етичний аспект цифрових прав вимагає відповідальності з боку держав корпорацій та громадянського суспільства, оскільки правове регулювання повинно не лише відповідати існуючим викликам, але й передбачати можливі ризики майбутнього технологічного розвитку. На цьому тлі, важливим є формування стандартів прозорості алгоритмів та впровадження механізмів незалежного аудиту для запобігання дискримінації та зловживань у цифровому просторі.

Аналізуючи перспективи подальшого дослідження цифрових прав, варто відзначити що однією з ключових задач є розробка глобальної нормативної бази, яка б регулювала діяльність технологічних гігантів, забезпечувала баланс між національною безпекою та правами людини, гарантувала ефективний захист персональних даних. Також необхідно розвивати технологічні рішення, які сприятимуть зміцненню цифрової безпеки серед таких інновацій. Також можна виокремити децентралізовані платформи, новітні методи шифрування та інструменти для аналізу й аудиту алгоритмічних рішень.

Загалом проблематика цифрових прав є однією з визначальних у контексті сучасних глобалізаційних процесів, адже питання приватності цифрової нерівності та етичного використання технологій впливають не лише на правову сферу, а й на соціальні, економічні та політичні аспекти розвитку суспільства. Тому, ефективно вирішення зазначених питань можливе лише за умови міжнародної співпраці, розробки універсальних стандартів та впровадження прогресивних технологій що забезпечать стабільність і справедливість у цифровому просторі.

Список літератури:

1. Cambridge Analytica scandal: how 87 million Facebook users had their data exploited. The Guardian. 2018. URL: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> (дата звернення: 13.02.2025).
2. Facebook to pay \$100 million to settle SEC charges for misleading investors. U.S. Securities and Exchange Commission. 2019. URL: <https://www.sec.gov/news/press-release/2019-140> (дата звернення: 13.02.2025).
3. Schneier, B. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World. W.W., 2021.
4. Guitton, C. Digital Privacy and the Protection of Data. Journal of Digital Information. 2020.
5. Binns, R. Algorithmic Bias and Its Impact on Society. 2022.
6. Zuboff, S. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs, 2019.
7. Floridi, L. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford University Press, 2014.

8. Crawford, K. Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence. Yale University Press, 2021.
9. Lessig, L. Code: And Other Laws of Cyberspace, Version 2.0. Basic Books, 2006.
10. Solove, D. J. The Digital Person: Technology and Privacy in the Information Age. NYU Press, 2008.
11. O'Neil, C. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Crown Publishing, 2016.
12. Tufekci, Z. Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency. Colorado Technology Law Journal. 2015.
13. European Commission. Artificial Intelligence Act: Proposal for a Regulation. 2022. URL: <https://surl.li/rpbajr> (дата звернення: 13.02.2025).
14. United Nations. The Role of the United Nations in Digital Rights Protection. UN Digital Economy Paper No. 65, 2021.
15. Тім Бернерс-Лі. URL: <https://surl.li/tpvhfn>
16. General Data Protection Regulation (GDPR). Official Journal of the European Union. 2016. URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> (дата звернення: 13.02.2025).
17. Google. Офіційний сайт компанії. URL: <https://www.google.com> (дата звернення: 13.02.2025).
18. Facebook. Офіційний сайт компанії. URL: <https://www.facebook.com> (дата звернення: 13.02.2025).
19. Amazon. Офіційний сайт компанії. URL: <https://www.amazon.com> (дата звернення: 13.02.2025).
20. Greenwald, G., MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 2013. URL: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (дата звернення: 13.02.2025).
21. The National Security Agency (NSA). Офіційний сайт. URL: <https://www.nsa.gov> (дата звернення: 13.02.2025).
22. Guitton, C. Digital Privacy and the Protection of Data. Journal of Digital Information, 21(1), 34–45.
23. Міжнародний союз електрозв'язку. Статистика розвитку інформаційно-комунікаційних технологій. Женева: ITU, 2021. URL: https://en.wikipedia.org/wiki/Internet_in_Africa (дата звернення: 19.02.2025).
24. Tech Today. Половина світу виходить в інтернет через мобільні пристрої. 2023. URL: <https://surl.li/gfqlj> (дата звернення: 19.02.2025).
25. United Nations High Commissioner for Human Rights. (2021). The right to privacy in the digital age. Report to the Human Rights Council. A/HRC/48/31. Retrieved.
26. Amazon. URL: <https://surl.li/hmmayx>
27. Чапліч С. Упереджений ШІ, або Як технології призводять до зростання випадків дискримінації, 2024. URL: <https://proit.ua/upieriedzhienii-shi-abo-ia-k-tiekhnologhiyi-prizvodiat-do-zrostannia-vypadkiv-diskriminatsiyi>. (дата звернення: 19.02.2025).
28. NetBlocks. Через масові протести в Ірані відключили інтернет і мобільний зв'язок. 2019. URL: https://lb.ua/world/2019/11/17/442491_izza_massovih_protestov_irane.html
29. Захист персональних даних за правилами GDPR. 2018/ URL: <https://ecpl.com.ua/news/zakhyst-personal-nukh-danykh-za-pravylamy-gdpr/>, вільний. (дата звернення: 19.02.2025).
30. Савченко В. Виклики щодо захисту інформації в хмарних середовищах / Актуальні проблеми кібербезпеки: матеріали Всеукраїнської науково-практичної конференції (м. Київ, 27 жовтня 2023 року). Київ: Державний університет інформаційно-комунікаційних технологій, 2023. С. 14–15.

Horielova V.Yu. DIGITAL RIGHTS: MORAL ASPECTS AND CHALLENGES

The article analyses the ethical and legal aspects of human rights protection in the context of global digitalisation. The article emphasises the relevance of the topic due to the rapid development of information technology, which creates new opportunities and threats to privacy, freedom of speech and equal access to digital resources.

The main issues discussed in the article are privacy violations, digital inequality, algorithmic bias, and the dominance of large technology companies (Big Tech). In particular, it analyses such high-profile cases as the Cambridge Analytica scandal, the PRISM programme, and cases of digital discrimination related to algorithmic systems, such as gender bias in Amazon's hiring algorithms.

The article emphasises the importance of developing a comprehensive approach to the protection of digital rights, including strengthening international regulation, developing technologies for personal data protection (VPN, encryption), ensuring transparency of algorithms and implementing ethical standards. Particular attention is paid to the ethical responsibility of states, corporations and civil society in creating a safe and fair digital environment.

The article uses an interdisciplinary approach that combines legal analysis, ethical research and the case study method. The analysis of international regulations, scientific publications, and practical examples made it possible to outline the main areas for improving legal and technological regulation in the field of digital rights.

The author concludes that it is necessary to harmonise legal norms at the global level, create international standards for regulating the activities of technology corporations, and actively develop technological solutions that will ensure data protection and prevent monopolisation of the digital space. The article also emphasises the importance of raising digital literacy among the population as one of the key factors in protecting digital rights.

Key words: Digital rights, legal regulation, ethical standards, digital security.