УДК 341.231.14:341.3:004.738.5
DOI https://doi.org/10.32782/TNU-2707-0581/2026.5/57

Тицька Я. О.
https://orcid.org/0000-0001-5777-8225
Міжнародний університет

ЗАХИСТ ПРАВ ЛЮДИНИ В УМОВАХ ІНФОРМАЦІЙНОЇ ВІЙНИ: МІЖНАРОДНО-ПРАВОВІ СТАНДАРТИ ТА МЕХАНІЗМИ

У статті досліджено міжнародно-правові стандарти захисту прав людини в умовах інформаційної війни та визначено межі правомірного реагування держав і цифрових платформ на дезінформацію, пропаганду війни та мову ненависті.

Розкрито взаємозв'язок свободи вираження поглядів, права на інформацію і приватність, заборони дискримінації та обов'язку держави захищати життя і безпеку людини.

Доведено, що інформаційна війна не утворює самостійної універсальної підстави для обмеження прав і свобод: кожне втручання має відповідати критеріям законності, легітимної мети, необхідності та пропорційності, а також враховувати контекст, статус поширювача, умисел, зміст і форму повідомлення, масштаб його поширення та ймовірність заподіяння шкоди.

Запропоновано чотирирівневу модель юридичної кваліфікації інформаційного впливу: правомірне, хоча й спірне висловлювання; системна дезінформація, що створює доведені суспільні ризики; пропаганда війни або підбурювання до дискримінації, ворожнечі чи насильства; пряме публічне підбурювання до геноциду. Для кожного рівня визначено пропорційний комплекс засобів реагування – від доступу до достовірної інформації, підтримки незалежних медіа, контрмовлення, медіаграмотності, маркування штучного контенту та демонетизації до обмеження алгоритмічного поширення, видалення матеріалів, санкцій і міжнародної кримінальної відповідальності.

Обґрунтовано необхідність поєднання матеріальних заборон із процесуальними гарантіями: незалежним контролем, мотивуванням рішень, повідомленням про підстави втручання, правом на оскарження, прозорістю алгоритмів, оцінюванням системних ризиків та збереженням цифрових доказів.

Окрему увагу приділено позитивним зобов'язанням держав щодо забезпечення інформаційного плюралізму, захисту журналістів і потерпілих, доступу до ефективних засобів юридичного захисту, а також міжнародному співробітництву у сфері виявлення, документування та припинення транскордонних інформаційних операцій, здатних завдати істотної шкоди демократичним інституціям і правам людини в умовах війни.

Сформульовано рекомендації щодо імплементації моделі в Україні з урахуванням воєнного стану, стандартів ООН, Ради Європи, ОБСЄ та права Європейського Союзу.

Ключові слова: *права людини, інформаційна війна, свобода вираження поглядів, дезінформація, пропаганда війни, мова ненависті, міжнародно-правові стандарти, цифрові платформи, міжнародна відповідальність, інформаційна безпека.*

Постановка проблеми. Цифровізація комунікації змінила не тільки швидкість поширення відомостей, а й архітектуру впливу на людину. Координовані кампанії здатні одночасно формувати викривлене уявлення про воєнні події, дегуманізувати групи населення, залякувати цивільних, підривати довіру до демократичних інституцій і перешкоджати реалізації права на вільне формування думки. Водночас посилання на інформаційну безпеку дедалі частіше використовується для надмірного блокування контенту, стеження, обмеження журналістики та придушення критики. Тому центральною є не дилема «безпека або свобода», а побудова такого механізму, який одночасно захищає особу від цілеспрямованої інформаційної шкоди і від свавільного державного чи приватного контролю над інформаційним простором.

© Тицька Я. О., 2026
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

Аналіз останніх досліджень і публікацій. Сучасні дослідження пропонують розмежовувати mis-information – помилкові відомості, поширені без наміру завдати шкоди; dis-information – свідомо неправдиві відомості, створені або поширені з таким наміром; та mal-information – справжні відомості, використані для заподіяння шкоди [1]. У міжнародно-правовій доктрині Б. Бааде показав обмеженість загальної заборони «фейкових новин» і небезпеку карати за тенденційне тлумачення фактів [2]. Г. Ламанн дослідив умови атрибуції транскордонних операцій з дезінформації державі та застосування норм про міжнародну відповідальність [3]. Натомість невирішеним залишається питання єдиної шкали кваліфікації різних форм інформаційного впливу та співвідношення заходів протидії з позитивними і негативними зобов'язаннями держав у сфері прав людини. Бракує також моделі, яка поєднувала б стандарти ООН, Ради Європи, ОБСЄ, Європейського Союзу та правила відповідальності за найтяжчі міжнародні злочини.

Постановка завдання. Метою статті є визначення змісту міжнародно-правових стандартів захисту прав людини в умовах інформаційної війни, установлення юридичних порогів для обмеження інформаційного контенту та формування правозахисної моделі реагування, придатної для імплементації в Україні.

Виклад основного матеріалу. Поняття «інформаційна війна» не закріплене в універсальному міжнародному договорі та не утворює автономного правового режиму, здатного змінювати обсяг міжнародних зобов'язань держав або автоматично легітимувати обмеження прав людини. Воно характеризує особливий контекст організованого, систематичного й переважно транскордонного інформаційного впливу, в межах якого поєднуються створення та поширення контенту, використання цифрової інфраструктури, алгоритмічне підсилення повідомлень, приховування джерел фінансування й координація діяльності різних суб'єктів. Тому юридична кваліфікація має ґрунтуватися не на політичному позначенні певного повідомлення як «ворожого», а на встановленні сукупності юридично значущих ознак: суб'єкта та його зв'язку з державою, характеру й спрямованості умислу, достовірності або маніпулятивності відомостей, способу їх поширення, масштабів охоплення, властивостей цільової аудиторії, причинного зв'язку з конкретною загрозою та тяжкості можливої шкоди. Такий підхід дає змогу розмежувати правомірну критику, журналістську помилку, добросовісне поширення неперевіреної інформації, координовану дезінформаційну операцію, пропаганду війни та підбурювання до насильства.

Необхідність такого розмежування зумовлена комплексним характером прав людини, яких може стосуватися інформаційний вплив. Повідомлення, що спрямовують насильство проти конкретних осіб або груп, створюють загрозу праву на життя й особисту безпеку; дегуманізуюча риторика посягає на принцип рівності та заборону дискримінації; доксинг, незаконне профілювання і мікротаргетинг втручаються у приватність та захист персональних даних; маніпулювання виборчою поведінкою впливає на право брати участь в управлінні державою; небезпечна медична дезінформація може перешкоджати реалізації права на здоров'я. Водночас надмірна протидія інформаційним загрозам здатна обмежувати свободу думки, свободу вираження поглядів, доступ до інформації, журналістську діяльність і політичний плюралізм. Звідси випливає подвійна природа міжнародно-правових зобов'язань держави: вона повинна утримуватися від свавільного втручання в інформаційну сферу і водночас забезпечувати належний захист осіб від передбачуваної інформаційно зумовленої шкоди. Проте позитивні зобов'язання не можуть тлумачитися як повноваження держави встановлювати обов'язкову для суспільства версію істини.

Вихідним нормативним орієнтиром залишається стаття 19 Міжнародного пакту про громадянські і політичні права, яка гарантує право шукати, одержувати й поширювати інформацію та ідеї незалежно від кордонів [4]. Втручання у здійснення цього права є допустимим лише за одночасної наявності передбаченої законом підстави, легітимної мети, доведеної суспільної необхідності та пропорційності обраного заходу. Закон має бути доступним і сформульованим із достатньою точністю, щоб особа могла передбачити правові наслідки своєї поведінки, а орган, який застосовує обмеження, не отримував необмеженої дискреції. Вимога необхідності передбачає встановлення прямого й безпосереднього зв'язку між конкретним висловлюванням і загрозою охоронюваному інтересу, тоді як пропорційність потребує доведення неможливості досягти поставленої мети менш обтяжливими засобами [5].

За такого підходу неправдивість повідомлення є юридично релевантною, але не самодостатньою ознакою. Вона може підтверджувати умисел, оманливий характер інформаційної поведінки

або передбачуваність шкоди, проте сама по собі не виправдовує криміналізації чи видалення контенту. Спеціальна доповідачка ООН з питань свободи думки та вираження обґрунтовано застерігає, що загальні заборони «фейкової інформації» створюють охолоджувальний ефект і дозволяють державним органам довільно визначати межі допустимого суспільного дискурсу [6]. Аналогічну позицію закріплено у Спільній декларації спеціальних мандатаріїв ООН, ОБСЄ, ОАД та Африканської комісії 2017 року: абстрактні заборони поширення «неправдивої» або «необ'єктивної» інформації несумісні з міжнародними стандартами, тоді як належними засобами реагування визнаються інформаційний плюралізм, доступ до офіційних даних, незалежна журналістика, спростування, корекція та медіаграмотність [7]. Міжнародне право, таким чином, охороняє не істину як установлений державою результат, а інституційні й процедурні умови її вільного суспільного пошуку.

Цей загальний принцип не виключає існування вузько визначених категорій висловлювань, заборона яких становить міжнародне зобов'язання держави. Відповідно до статті 20 Пакту законом повинні заборонятися пропаганда війни та виступи на користь національної, расової чи релігійної ненависті, які є підбурюванням до дискримінації, ворожнечі або насильства [4]. Застосування цієї норми не усуває гарантій статті 19: законодавчий склад правопорушення має бути визначеним, а обмеження – необхідним, пропорційним та індивідуалізованим [5]. Рабатський план дій конкретизує цей підхід через оцінювання соціально-політичного контексту, статусу і впливу промовця, спрямованості його умислу, змісту та форми повідомлення, масштабів поширення й імовірності настання шкоди [8]. Значення такого тесту полягає у недопустимості підміни доказування реальної небезпеки посиланням лише на різкість, образливість або політичну неприйнятність висловлювання.

Граничним проявом протиправного інформаційного впливу є пряме й публічне підбурювання до геноциду, криміналізоване Конвенцією про запобігання злочину геноциду та Римським статутом Міжнародного кримінального суду [9; 10]. Практика Міжнародного кримінального трибуналу щодо Руанди у справі Nahimana та інші підтвердила, що медіакомунікація може породжувати індивідуальну міжнародну кримінальну відповідальність, якщо вона містить безпосередній заклик до знищення захищеної групи [11]. Водночас критерій прямого підбурювання повинен застосовуватися з урахуванням мовного, культурного та суспільного контексту. Це унеможливлює механічне прирівнювання будь-якої ворожої пропаганди до міжнародного злочину, не применшуючи обов'язку держави своєчасно реагувати на висловлювання, здатні спричинити масове насильство.

Універсальні стандарти отримують подальшу конкретизацію в європейському правовому просторі. Стаття 10 Європейської конвенції з прав людини охоплює як поширення, так і одержання інформації, а допустимість втручання пов'язує з його необхідністю в демократичному суспільстві [12]. Рекомендація CM/Rec(2022)16 Комітету міністрів Ради Європи розвиває диференційований підхід до мови ненависті, відповідно до якого кримінально-правові заходи мають застосовуватися до найтяжчих форм, цивільні й адміністративні засоби – до менш небезпечних проявів, а освіта, контрмовлення, підтримка потерпілих і саморегулювання – виконувати превентивну функцію [13]. Під час війни контекст може істотно підвищувати передбачуваність насильства, але не звільняє державу від обов'язку встановити умисел, характер підбурювання та ймовірність шкоди.

Важливим для визначення меж відповідальності інформаційних посередників є рішення Великої палати Європейського суду з прав людини у справі Sanchez v. France. Суд не встановив порушення статті 10 Конвенції у зв'язку з притягненням політика до відповідальності за несвоєчасне видалення явно протиправних коментарів третіх осіб на публічній сторінці, яка використовувалася у виборчій кампанії [14]. Проте це рішення не встановлює загального обов'язку попередньо контролювати всі висловлювання користувачів. Його правове значення полягає в контекстній оцінці професійного статусу власника сторінки, передбачуваності ризику, характеру коментарів, масштабів аудиторії та фактичної можливості оперативно відреагувати. Отже, відповідальність посередника має ґрунтуватися не на самому факті розміщення чужого матеріалу, а на поєднанні знання про його очевидну незаконність, реального контролю над поширенням і бездіяльності після отримання належного повідомлення.

Розвиток цифрових платформ зумовив поступовий перехід від моделі реагування на окремий протиправний матеріал до регулювання системних ризиків інформаційної екосистеми. Регламент (ЄС) 2022/2065 про цифрові послуги покладає на дуже великі онлайн-платформи обов'язок оцінювати та зменшувати ризики для основоположних прав, громадянського дискурсу, виборчих про-

цесів і громадської безпеки, забезпечувати прозорість реклами, модерації та рекомендаційних систем, а також проходити незалежний аудит [15]. Регламент (ЄС) 2024/1689 про штучний інтелект доповнює цю модель вимогами щодо розкриття штучного походження або маніпулювання deepfake-зображеннями, аудіовізуальними матеріалами та, у визначених випадках, текстами суспільного інтересу [16]. Юридична цінність такого підходу полягає в перенесенні уваги з покарання окремого користувача на архітектуру сервісу, яка визначає швидкість, масштаб і адресність поширення контенту.

Водночас покладення регуляторних обов'язків на платформи створює ризик приватизованої цензури. Якщо загроза значної санкції спонукає оператора превентивно видаляти сумнівний, але законний матеріал, держава фактично досягає обмежувального результату без дотримання процесуальних гарантій. Тому платформне регулювання має передбачати оприлюднені й доступні правила, мотивоване повідомлення про підставу рішення, внутрішню процедуру оскарження, можливість позасудового вирішення спору, судовий контроль і статистичну прозорість. Керівні принципи ООН з питань бізнесу і прав людини вимагають від компаній здійснювати належну обачність, запобігати негативному впливу на права людини, пом'якшувати його наслідки та сприяти відновленню порушених прав, у тому числі в умовах збройного конфлікту [17]. Керівні принципи ЮНЕСКО з урядування цифрових платформ розвивають цю вимогу через багатосторонню, незалежну й засновану на правах людини модель регулювання [18].

Поряд із захистом прав людини інформаційна війна має міждержавний вимір. Транскордонна дезінформаційна операція за певних обставин може порушувати принцип невтручання, суверенітет, міжнародні зобов'язання у сфері прав людини або спеціальні договірні режими. Для виникнення міжнародної відповідальності необхідно встановити можливість присвоєння відповідної поведінки державі та порушення конкретного первинного міжнародного зобов'язання [3]. Так само державне фінансування медіа або політична вигідність поширюваного наративу не завжди доводять здійснення державою ефективного контролю над конкретною інформаційною операцією.

Особливо складним залишається застосування принципу невтручання, оскільки його порушення передбачає наявність примусового впливу на сферу, в якій держава зберігає свободу політичного вибору. Тому приховане формування громадської думки, навіть якщо воно має ворожий і маніпулятивний характер, не в кожному випадку досягає порогу забороненого втручання. Необхідно довести зв'язок між інформаційною операцією та фактичним позбавленням держави можливості вільно здійснювати свої суверенні повноваження. Це зумовлює потребу поєднувати технічну атрибуцію, встановлення організаційних і фінансових зв'язків, документування ланцюга командування, збереження метаданих і міжнародну правову допомогу, не знижуючи належного стандарту доказування.

Справа RT France v. Council демонструє можливість застосування цільових обмежувальних заходів у винятковому контексті воєнної агресії. Загальний суд ЄС визнав пропорційним тимчасове обмеження мовлення, врахувавши спрямованість діяльності медіа на пропагандистську підтримку агресії, часову обмеженість заходу та наявність судового контролю [19]. Водночас це рішення не може тлумачитися як загальний дозвіл на постійне блокування іноземних засобів масової інформації за критерієм їхнього походження. Орган, який застосовує обмеження, повинен довести функціональний зв'язок між конкретною діяльністю мовника, загрозою, яку належить усунути, і поставленою правомірною метою, оцінити менш обмежувальні альтернативи та забезпечити регулярний перегляд рішення.

Системне узагальнення розглянутих міжнародно-правових стандартів дає змогу запропонувати диференційовану модель кваліфікації інформаційного впливу, засновану не на формальному поділі контенту на «правильний» і «неправильний», а на послідовному підвищенні юридично значущого ризику. Вихідну межу цієї моделі утворюють оцінні судження, критика, сатира, спірні інтерпретації та добросовісні фактичні помилки. Вони перебувають під повним захистом свободи вираження, а реагування держави повинно обмежуватися забезпеченням доступу до першоджерел, підтримкою незалежної журналістики, фактчекінгом, контрмовленням і розвитком медіаграмотності.

Наступне положення у цій нормативній градації займає системна дезінформація, яка свідомо та координовано поширюється у значному масштабі й створює доведений ризик для прав людини, виборчих процесів, громадського здоров'я або безпеки, але не досягає порогу підбурювання. У такому випадку пріоритетними є розкриття походження матеріалів, позначення штучно ство-

реного контенту, зменшення алгоритмічного підсилення, демонетизація, прозорість політичної реклами, повідомлення користувачів і поширення перевіреної інформації. Видалення допускається лише за наявності додаткової законної підстави, оскільки сама належність матеріалу до дезінформаційної кампанії не скасовує вимоги індивідуальної оцінки.

Коли інформаційна поведінка набуває ознак пропаганди війни або підбурювання до дискримінації, ворожнечі чи насильства, виникає обов'язок застосувати статтю 20 Пакту і пороговий тест Рабатського плану дій. Оперативне припинення поширення, адміністративна або кримінальна відповідальність є допустимими лише за умови точного законодавчого визначення складу правопорушення, доведення умислу й високої ймовірності шкоди та забезпечення повного комплексу процесуальних гарантій. На граничній точці цієї моделі перебуває пряме й публічне підбурювання до геноциду, яке активує міжнародні обов'язки запобігання, розслідування, переслідування винних та міжнародного співробітництва. Невідкладне припинення доступу до відповідних матеріалів повинно супроводжуватися збереженням їх автентичних копій, метаданих і ланцюга зберігання для подальшого використання як доказів.

Практичне застосування запропонованої моделі передбачає послідовну юридичну процедуру. Компетентний орган має спочатку встановити факти, відокремити оцінне судження від фактичного твердження, визначити характер інформаційної поведінки та наявність координованого поширення. Після цього перевіряються законність втручання, його легітимна мета, необхідність і пропорційність, а щодо ненависницьких висловлювань – також критерії Рабатського плану. Обраний захід повинен бути найменш обмежувальним серед тих, що здатні ефективно усунути доведену загрозу. Рішення має містити фактичне і правове обґрунтування, визначений строк дії, порядок оскарження та можливість незалежного судового контролю. Завершальним елементом є оцінювання результативності заходу та його побічного впливу на журналістику, політичну опозицію, меншинні групи й суспільний дискурс. Саме така процедура перетворює пропорційність із загального принципу на практично перевірюваний стандарт.

В Україні нормативну основу відповідного механізму становлять стаття 34 Конституції України [20], закони України «Про інформацію» [21] і «Про медіа» [22], а також Стратегія інформаційної безпеки [23]. Воєнний стан об'єктивно посилює необхідність захищати оперативну інформацію, цивільне населення й обороноздатність держави, однак не усуває вимог законності, недискримінації, суворої необхідності та доступу до ефективного засобу юридичного захисту. Тимчасові обмеження повинні бути пов'язані з конкретною загрозою, мати визначений строк, регулярно переглядатися та припинятися після зникнення підстав. Вони не можуть перетворюватися на загальну заборону критики державної політики або на інструмент контролю за суспільною дискусією.

Удосконалення національного законодавства доцільно спрямовувати не на запровадження універсального правопорушення «дезінформація», а на визначення диференційованих складів, пов'язаних із конкретною охоронюваною шкодою. Критерії державних обмежень і звернень до цифрових платформ повинні бути публічними, а кожне рішення – містити фактичне та правове обґрунтування, строк дії і порядок оскарження. Невідкладне блокування має підлягати подальшому незалежному, переважно судовому, контролю. Для великих цифрових платформ необхідними є оцінювання системних ризиків для прав людини, надання дослідникам доступу до належно захищених даних, оприлюднення звітів про українськомовну модерацію та незалежний аудит рекомендаційних систем.

Самостійним складником механізму має стати збереження цифрових доказів. Первинний файл, часові позначки, ідентифікатори акаунтів, відомості про редагування, масштаби охоплення, рекламне фінансування та зв'язки координованої мережі повинні фіксуватися з дотриманням вимог приватності, автентичності та безперервності ланцюга зберігання. Видалення матеріалу без належного архівування може позбавити потерпілих доказів, ускладнити встановлення державної атрибуції та перешкодити розслідуванню міжнародних злочинів. Тому співробітництво України з ООН, ОБСЄ, Радою Європи, Європейським Союзом і Міжнародним кримінальним судом має поєднувати раннє попередження, обмін доказовою інформацією, підтримку незалежних медіа, захист журналістів і розвиток належної обачності цифрових платформ. Спільна заява міжнародних мандатаріїв щодо вторгнення в Україну підтверджує, що протидія дезінформації повинна здійснюватися у взаємозв'язку з прозорістю, підзвітністю та міжнародними стандартами свободи вираження [24].

Висновки. Проведене дослідження дає підстави стверджувати, що інформаційна війна є обставиною підвищеного ризику для прав людини, але не самостійною універсальною підставою для обмеження свободи вираження. Міжнародно-правовий механізм має захищати людину у двох напрямах: від маніпуляції, підбурювання, дискримінації та насильства і від свавільної цензури, стеження та непрозорої платформної модерації.

Запропонована чотирирівнева модель відокремлює правомірне висловлювання, системну дезінформацію з доведеним ризиком, заборонене підбурювання або пропаганду війни та пряме публічне підбурювання до геноциду. Її практичне значення полягає у відповідності кожного рівня окремому набору заходів: від контрмовлення і прозорості до обмеження поширення, санкцій та міжнародної кримінальної відповідальності. Обов'язковою частиною механізму є процедура – точний закон, доказування умислу й ризику, найменш обмежувальний засіб, мотивоване рішення, часові межі, незалежне оскарження, алгоритмічна прозорість і збереження доказів.

Для України пріоритетними є гармонізація інформаційного законодавства зі статтями 19 і 20 Пакту та статтею 10 Конвенції, запровадження судового контролю за невідкладними блокуваннями, правозахисна оцінка платформних ризиків, підтримка незалежної журналістики й інституційна співпраця щодо доказування транскордонних інформаційних операцій. Подальші дослідження мають бути спрямовані на стандарти атрибуції алгоритмічно підсилених операцій та критерії причинного зв'язку між цифровим контентом і шкодою правам людини.

Список літератури:

1. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report DGI(2017)09. Strasbourg, 2017. 109 p. URL: https://rm.coe.int/information-disorder-report/1680764666.

2. Baade B. Fake News and International Law. *European Journal of International Law.* 2018. Vol. 29, Issue 4. P. 1357–1376. DOI: https://doi.org/10.1093/ejil/chy071.

3. Lahmann H. Infecting the Mind: Establishing Responsibility for Transboundary Disinformation. *European Journal of International Law.* 2022. Vol. 33, Issue 2. P. 411–440. DOI: https://doi.org/10.1093/ejil/chac023.

4. International Covenant on Civil and Political Rights, 16 December 1966. *United Nations, Treaty Series*. Vol. 999. URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

5. General Comment No. 34: Article 19: Freedoms of Opinion and Expression. CCPR/C/GC/34. 12 September 2011. URL: https://www.ohchr.org/sites/default/files/english/bodies/hrc/docs/gc34.pdf.

6. Disinformation and Freedom of Opinion and Expression: Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. A/HRC/47/25. 13 April 2021. URL: https://undocs.org/A/HRC/47/25.

7. Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda. 3 March 2017. URL: https://www.osce.org/files/f/documents/6/8/302796.pdf.

8. Human Rights Council. Rabat Plan of Action on the Prohibition of Advocacy of National, Racial or Religious Hatred that Constitutes Incitement to Discrimination, Hostility or Violence. A/HRC/22/17/Add.4. 11 January 2013. URL: https://undocs.org/A/HRC/22/17/Add.4.

9. Convention on the Prevention and Punishment of the Crime of Genocide, 9 December 1948. *United Nations, Treaty Series.* Vol. 78. URL: https://www.un.org/en/genocide-prevention/1948-convention.

10. Rome Statute of the International Criminal Court, 17 July 1998. *United Nations, Treaty Series.* Vol. 2187. URL: https://www.icc-cpi.int/sites/default/files/Publications/Rome-Statute.pdf.

11. Prosecutor v. Nahimana, Barayagwiza and Ngeze. Judgment. ICTR-99-52-A. Appeals Chamber. 28 November 2007. URL: https://unictr.irmct.org/sites/unictr.org/files/case-documents/ictr-99-52/appeals-chamber-judgements/en/071128.pdf.

12. Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950. *European Treaty Series.* No. 5. URL: https://www.echr.coe.int/documents/d/echr/convention_ukr.

13. Recommendation CM/Rec(2022)16 of the Committee of Ministers to Member States on Combating Hate Speech. 20 May 2022. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680a67955.

14. Sanchez v. France [GC], no. 45581/15, ECHR, 15 May 2023. URL: https://hudoc.echr.coe.int/eng?i=001-224928.

15. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. *Official Journal of the European Union*. 2022. L 277. P. 1–102. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

16. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence. *Official Journal of the European Union.* 2024. L, 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

17. Guiding Principles on Business and Human Rights. New York; Geneva, 2011. URL: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf.

18. Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach. Paris, 2023. 58 p. URL: https://unesdoc.unesco.org/ark:/48223/pf0000387339.

19. RT France v Council, T-125/22, Judgment of the General Court (Grand Chamber), 27 July 2022, ECLI:EU:T:2022:483. URL: https://curia.europa.eu/juris/liste.jsf?num=T-125/22.

20. Конституція України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр.

21. Про інформацію: Закон України від 2 жовтня 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.

22. Про медіа: Закон України від 13 грудня 2022 р. № 2849-IX. URL: https://zakon.rada.gov.ua/laws/show/2849-20.

23. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069.

24. Joint Statement on the Russian Federation's Invasion of Ukraine and the Importance of Freedom of Expression and Information. 4 March 2022. URL: https://www.osce.org/representative-on-freedom-of-media/513459.

Titska Ya. O. PROTECTION OF HUMAN RIGHTS IN THE CONTEXT OF INFORMATION WARFARE: INTERNATIONAL LEGAL STANDARDS AND MECHANISMS

The article examines international legal standards for the protection of human rights in the context of information warfare and determines the limits of lawful responses by states and digital platforms to disinformation, propaganda for war, and hate speech.

It reveals the interrelationship between freedom of expression, the rights to information and privacy, the prohibition of discrimination, and the state's obligation to protect human life and security.

It is argued that information warfare does not constitute an independent universal ground for restricting human rights and freedoms: every interference must satisfy the criteria of legality, legitimate aim, necessity, and proportionality, while also taking into account the context, the status of the disseminator, intent, the content and form of the communication, the scale of its dissemination, and the likelihood of harm.

A four-level model for the legal classification of information influence is proposed: lawful, albeit controversial, expression; systemic disinformation creating demonstrated societal risks; propaganda for war or incitement to discrimination, hostility, or violence; and direct public incitement to genocide.

A proportionate set of response measures is identified for each level, ranging from access to reliable information, support for independent media, counter-speech, media literacy, labelling of artificially generated content, and demonetisation to restrictions on algorithmic dissemination, content removal, sanctions, and international criminal responsibility.

The article substantiates the need to combine substantive prohibitions with procedural safeguards, including independent oversight, reasoned decisions, notification of the grounds for interference, the right to appeal, algorithmic transparency, systemic risk assessment, and the preservation of digital evidence.

Particular attention is paid to the positive obligations of states to ensure information pluralism, protect journalists and victims, provide access to effective legal remedies, and promote international cooperation in detecting, documenting, and terminating cross-border information operations capable of causing significant harm to democratic institutions and human rights during wartime.

Recommendations are formulated for implementing the proposed model in Ukraine, taking into account martial law, the standards of the United Nations, the Council of Europe and the OSCE, and European Union law.

Keywords: *human rights, information warfare, freedom of expression, disinformation, propaganda for war, hate speech, international legal standards, digital platforms, international responsibility, information security.*

Дата першого надходження статті до видання: 02.09.2026
Дата прийняття статті до друку після рецензування: 15.09.2026
Дата публікації (оприлюднення) статті: 18.11.2026