

УДК 340.13

DOI <https://doi.org/10.24144/2307-3322.2025.89.1.20>

ЗАКОНОДАВЧІ МЕХАНІЗМИ КОНТРОЛЮ НАД ІНФОРМАЦІЙНИМ ПРОСТОРОМ В ІНФОРМАЦІЙНИХ АВТОКРАТІЯХ: ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ

Саміло Г.,
*кандидат юридичних наук, доцент,
доцент кафедри конституційного,
адміністративного та трудового права
Національного університету «Запорізька політехніка»
ORCID: 0000-0001-9493-8013*

Романцов Ю.,
*аспірант кафедри конституційного,
адміністративного та трудового права
Національного університету «Запорізька політехніка»
ORCID: 0009-0003-4032-3365*

Саміло Г., Романцов Ю. Законодавчі механізми контролю над інформаційним простором в інформаційних автократіях: теоретико-правовий аналіз.

У статті здійснено комплексний аналіз законодавчих механізмів контролю над інформаційним простором у державах, які класифікуються як інформаційні автократії. Розглядається феномен інформаційної автократії як нової форми авторитарного режиму, що не обмежується класичним цензуруванням, а застосовує більш гнучкі, правові й технологічні інструменти для контролю над потоками інформації. Особливу увагу приділено законодавчим ініціативам і правовим нормам, що декларують захист національної безпеки, протидію дезінформації або інформаційному тероризму, але водночас використовуються для обмеження свободи слова, придушення опозиційних поглядів та монополізації публічного дискурсу. Під законодавчими механізмами контролю над інформаційним простором розуміється сукупність нормативно-правових актів, що регулюють доступ громадян до інформації, встановлюють обмеження свободи слова, накладають цензуру або передбачають можливості для блокування інформаційних ресурсів. У роботі виокремлено ключові механізми, зокрема прийняття законів про «фейкові новини», законодавче регулювання соціальних мереж, створення державних реєстрів заборонених сайтів, обов'язкову ідентифікацію користувачів онлайн-простору, а також інструменти непрямого впливу – як-от фінансовий тиск на ЗМІ, надання ліцензій, контроль за технічною інфраструктурою. Проаналізовано приклади з практики окремих країн, які впровадили комплексне інформаційно-правове регулювання для забезпечення політичного домінування чинної влади. Увагу приділено також юридичним суперечностям і колізіям між національними нормами таких країн та міжнародними стандартами в галузі прав людини. Мета статті – проаналізувати основні законодавчі механізми, що забезпечують функціонування інформаційної автократії, визначити їх особливості та наслідки для правового статусу особи. Об'єктом дослідження є інформаційний простір в умовах авторитарного політичного режиму (інформаційної автократії), що перебуває під контролем держави. Предметом дослідження є законодавчі механізми регулювання і контролю інформаційного простору в інформаційних автократіях, а також їхній вплив на свободу слова, цифрові права громадян та правовий статус особи. Методологія дослідження включає методологічні підходи (діяльнісний, системний, порівняльний, аксіологічний), загальнонаукові методи мислення (аналіз, синтез, абстрагування, узагальнення), філософські (діалектичний, метафізичний, герменевтичний, гносеологічний), загальнонаукові (історичний, синергетичний, функціональний, структурний) і конкретно науковий (формально-юридичний, порівняльно-правовий) методи. У результаті дослідження проаналізовано законодавчі механізми в інформаційних автократіях, які є частиною гібридної моделі

управління, що поєднує елементи формального демократичного регулювання з авторитарними практиками, спрямованими на збереження політичної стабільності, централізацію контролю та формування необхідного інформаційного середовища.

Ключові слова: інформаційна автократія, контроль над інформацією, свобода слова, інформаційна безпека, законодавчі механізми, авторитаризм.

Samilo H., Romantsov Yu. Legislative mechanisms of control over information space in information autocracies: theoretical and legal analysis.

The article presents a comprehensive analysis of legislative mechanisms for controlling the information space in states classified as informational autocracies. The phenomenon of informational autocracy is examined as a new form of authoritarian regime that does not rely solely on classical censorship but employs more flexible legal and technological instruments to manage information flows. Particular attention is given to legislative initiatives and legal norms that formally declare the protection of national security, the fight against disinformation or information terrorism, yet are simultaneously used to restrict freedom of speech, suppress opposition views, and monopolize public discourse.

Legislative mechanisms of information space control are understood as a set of normative legal acts regulating citizens' access to information, imposing restrictions on freedom of speech, applying censorship, or enabling the blocking of information resources. The paper identifies key mechanisms, including the adoption of laws on «fake news», legal regulation of social networks, creation of state registries of banned websites, mandatory user identification in the online space, and indirect tools such as financial pressure on the media, licensing requirements, and control over technical infrastructure.

The study analyzes practices from specific countries that have implemented comprehensive information-legal regulations to ensure the political dominance of the ruling regime. Attention is also given to legal conflicts and inconsistencies between national laws and international human rights standards. The purpose of the article is to analyze the main legislative mechanisms ensuring the functioning of informational autocracy, to define their features, and assess their consequences for the legal status of the individual.

The object of the research is the information space under an authoritarian political regime (informational autocracy) controlled by the state. The subject of the research is the legislative mechanisms for regulating and controlling the information space in informational autocracies, as well as their impact on freedom of speech, digital rights, and the legal status of the individual.

The methodology includes methodological approaches (activity-based, systemic, comparative, axiological), general scientific methods of reasoning (analysis, synthesis, abstraction, generalization), philosophical methods (dialectical, metaphysical, hermeneutic, epistemological), general scientific (historical, synergetic, functional, structural), and specific legal (formal-legal, comparative-legal) methods. As a result of the study, legislative mechanisms in informational autocracies are analyzed as part of a hybrid governance model combining elements of formal democratic regulation with authoritarian practices aimed at maintaining political stability, centralizing control, and shaping a controlled information environment.

Key words: informational autocracy, information control, freedom of speech, information security, legislative mechanisms, authoritarianism.

Постановка проблеми. В умовах розвитку цифрових технологій інформація перетворилася на один із найцінніших ресурсів сучасного суспільства. Це, своєю чергою, зумовило трансформацію форм політичного контролю. Одним із проявів такої трансформації є виникнення феномену інформаційної автократії – політичного режиму, в основі якого лежить централізоване керування потоками інформації, маніпулювання суспільною думкою та обмеження доступу громадян до альтернативних джерел знань. Особливої актуальності ця проблема набуває в контексті правового забезпечення такого контролю, адже саме законодавчі механізми створюють формальні підстави для функціонування інформаційної автократії.

Мета дослідження – проаналізувати основні законодавчі механізми, що забезпечують функціонування інформаційної автократії, визначити їх особливості та наслідки для правового статусу особи.

Стан опрацювання проблематики. Хоча проблема інформаційної автократії широко обговорюється в політологічних та медіазнавчих колах, у сфері теоретико-правових досліджень вона

залишається недостатньо вивченою. Існуючі праці переважно торкаються окремих аспектів – аналізу свободи слова, правового регулювання інтернету чи особливостей цензури, але комплексного правового аналізу механізмів побудови інформаційних автократій досі бракує. Водночас вивчення цих питань є важливим для розуміння того, як сучасні держави використовують законодавчі інструменти для встановлення контролю над суспільним дискурсом.

Виклад основного матеріалу. Під законодавчими механізмами контролю над інформаційним простором слід розуміти сукупність нормативно-правових актів, що регулюють доступ громадян до інформації, встановлюють обмеження свободи слова, накладають цензуру або передбачають можливості для блокування інформаційних ресурсів. Такі механізми можуть бути як відкритими й офіційно закріпленими (наприклад, закони про державну безпеку, боротьбу з екстремізмом, фейковими новинами), так і завуальованими через розпливчасті формулювання, що дозволяють широке тлумачення з боку державних органів.

Одним із типових інструментів є прийняття законів, що встановлюють обов'язок реєстрації медіа, контролю за ліцензіями, моніторинг контенту та санкції за «порушення стандартів». Іншим поширеним підходом є ухвалення норм, що передбачають кримінальну або адміністративну відповідальність за поширення «неправдивої інформації», «образу держави» чи «підрив суспільної моралі», залишаючи водночас широкий простір для суб'єктивної оцінки змісту висловлювань.

Інструменти такого контролю часто маскуються під забезпечення національної безпеки, боротьбу з тероризмом або захист громадян від дезінформації. Проте на практиці вони створюють передумови для вибіркового переслідування інакодумців та обмеження критичних висловлювань, що суперечить базовим принципам демократичної держави і прав людини.

Особливо небезпечним є поєднання законодавчих норм із технічними засобами впливу на інформаційний простір: впровадженням систем моніторингу інтернету, обов'язкового зберігання даних провайдерами, фільтрації контенту та блокування сайтів без рішення суду.

Отже, законодавчі механізми контролю над інформацією слугують не лише правовим оформленням політичного впливу, а й інструментом створення умов для самозбереження влади шляхом контролю за свідомістю громадян.

Одним із характерних прикладів законодавчих механізмів інформаційного контролю є розширення повноважень державних органів у сфері регулювання цифрового середовища. Законодавство, яке запроваджує обов'язкову ідентифікацію користувачів у мережі, встановлює вимоги до зберігання особистих даних або зобов'язує платформи передавати інформацію про своїх користувачів на вимогу влади, створює передумови для тотального нагляду. В умовах інформаційної автократії подібні норми оформлюються під виглядом необхідності забезпечення кібербезпеки чи боротьби з кіберзлочинністю, однак фактично перетворюються на інструмент контролю за суспільною активністю.

Ще одним важливим аспектом є впровадження законів про «інформаційний суверенітет» – концепцію, що дозволяє державі обмежувати або блокувати зовнішні інформаційні потоки, встановлювати «національні сегменти» інтернету, примушуючи глобальні технологічні компанії працювати за внутрішніми правилами або під загрозою санкцій. Хоча така політика нерідко обґрунтовується необхідністю захисту інформаційної безпеки та культурної самобутності, її реальним наслідком є ізоляція громадян від альтернативних джерел інформації, зміцнення монополії державних або лояльних медіа на формування суспільної думки. Прикладами таких законів є Cybersecurity Law of the People's Republic of China (діє з 1 червня 2017 р. та встановлює повний державний контроль за IT-інфраструктурою; зобов'язує компанії проходити «національну перевірку безпеки»; забороняє передавати дані за межі КНР без дозволу) [1]; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (зобов'язує соцмережі призначати представників в Індії; вимагає від месенджерів ідентифікувати «першоджерело повідомлення»; передбачає видалення контенту за 36 годин після запиту влади) [2]; Закон № 5651 «Про регулювання інтернет-публікацій» (Туреччина, 2007 р., із поправками 2020 р.) (вимагає від іноземних платформ мати юридичного представника в Туреччині; встановлює обов'язок видалення «незаконного контенту» протягом 48 годин) [3]. Схожі закони та підзаконні нормативні акти існують в РФ, Білорусі, Ірані.

Правовий аналіз показує, що законодавчі механізми інформаційного контролю мають системний характер і охоплюють кілька рівнів регулювання: правила доступу до інформації (реєстрація ЗМІ, ліцензування, заборона певних типів контенту); правила розповсюдження інформації

(контроль за змістом повідомлень, обмеження тем); правила споживання інформації (моніторинг користувацької активності, технології фільтрації контенту).

У багатьох країнах подібні норми були введені через еволюційний процес: спочатку шляхом м'якого регулювання, потім через запровадження штрафів та санкцій, і, нарешті, через створення адміністративних структур, відповідальних за контроль за дотриманням цих норм.

Особливу увагу в межах інформаційної автократії приділяють також так звані закони про «національні інтереси», які дозволяють обмежувати або забороняти діяльність ЗМІ, інтернет-платформ чи окремих осіб під приводом захисту державного суверенітету. Через розмитість понять, закладених у таких законах, вони стають інструментом вибіркового застосування права – коли рішення про порушення чи загрозу ухвалюються не на підставі об'єктивних критеріїв, а відповідно до політичної доцільності.

Таким чином, законодавчі механізми інформаційного контролю є не випадковими або ізольованими рішеннями, а елементами загальної стратегії зі зведення інформаційного простору під контроль політичної влади. Це формує основу для розвитку інших складових інформаційної автократії, таких як цензура, пропаганда і контроль над соціальними мережами.

Аналізуючи законодавчі механізми функціонування інформаційної автократії, важливо звернути увагу на використання технологічних інструментів у поєднанні з правовими нормами. В епоху цифровізації одне лише прийняття обмежувальних законів не забезпечує повного контролю над інформаційними потоками. Тому держава активно використовує технології: системи глибокої інспекції пакетів (Deep Packet Inspection, DPI), алгоритми штучного інтелекту для відстеження змісту повідомлень, автоматизовані фільтри для блокування контенту, бази даних спостереження за інтернет-активністю громадян.

Для легітимації застосування таких технологій держава часто приймає окремі нормативно-правові акти або вводить спеціальні режими. Наприклад, надзвичайний стан у цифровому просторі може бути підставою для введення масового моніторингу трафіку, відключення доступу до окремих сервісів або застосування санкцій до платформ, які відмовляються співпрацювати з державними органами.

У низці країн також функціонують реєстри заборонених сайтів та мобільних додатків, що юридично оформлюються відповідними списками, які підлягають обов'язковому виконанню інтернет-провайдерів. Показовим є те, що самі критерії включення до такого списку часто залишаються розмитими або взагалі не публікуються, що створює можливості для зловживань.

Окремий інтерес становлять закони, що вводять так звану «корпоративну відповідальність» цифрових платформ. У межах цих норм великі технологічні компанії зобов'язані самостійно фільтрувати контент, співпрацювати з державними органами, зберігати дані користувачів і забезпечувати їх доступ за запитом влади. Невиконання вимог тягне за собою суттєві штрафи або заборону діяльності на території країни. Таким чином, держава не лише здійснює прямий контроль, а й перекладає відповідальність за цензуру на приватні компанії, що ускладнює фіксацію порушень прав громадян.

Серед додаткових механізмів законодавчого впливу можна також відзначити: введення обов'язкового ліцензування для певних видів інтернет-діяльності (наприклад, для блогерів із великою аудиторією); заборону анонімності у мережі через вимоги до верифікації особистості; нормативне закріплення поняття «цифрового громадянства» із відповідними обмеженнями доступу до цифрових сервісів для невідповідних осіб.

Таким чином, законодавчі механізми інформаційної автократії базуються на комплексній взаємодії нормативних приписів, технологічних засобів та адміністративного тиску. Вони створюють ситуацію, за якої формальна легальність правових норм маскує фактичне порушення фундаментальних прав і свобод, унеможливаючи ефективний спротив громадян та незалежних медіа.

Системне застосування законодавчих механізмів інформаційного контролю призводить до глибоких трансформацій у правовому полі держави. Перш за все, формується особливий режим правового регулювання інформаційної сфери, який характеризується розмитістю норм, вибірковістю правозастосування та фактичним підпорядкуванням права політичній доцільності. Законодавство у таких умовах втрачає свою основну функцію – бути гарантом прав і свобод – і перетворюється на інструмент їхнього обмеження.

Характерною рисою законодавчого оформлення інформаційної автократії є створення широкого простору для дискреції державних органів. Закони часто формулюються настільки невизначено,

чено, що дозволяють владі самостійно визначати, яка інформація є «небажаною», «екстремістською», «фейковою» чи «загрозливою для національної безпеки». Така невизначеність підриває принцип правової визначеності, який є базовим у концепції верховенства права.

Крім того, важливо підкреслити тенденцію до скорочення судового контролю над обмеженнями свободи інформації. У ряді випадків передбачено можливість блокування сайтів, видалення контенту чи обмеження доступу без попереднього судового розгляду, лише на підставі адміністративного рішення спеціального органу. Це не лише суперечить принципу поділу влад, а й істотно знижує рівень гарантій захисту прав громадян.

У межах інформаційної автократії виникає й особливе процесуальне право, яке регулює розгляд справ, пов'язаних із порушенням інформаційних норм. Такі справи часто розглядаються у спрощеному порядку, без забезпечення повноцінної змагальності сторін або доступу до справедливого судового захисту. У деяких країнах навіть створюються спеціалізовані суди чи квазісудові органи, що займаються розглядом «інформаційних правопорушень», що ще більше посилює тенденцію до автономізації інформаційного права в межах автократичної системи.

Законодавче оформлення інформаційної автократії має і глибокі міжнародні наслідки. Багато норм внутрішнього права суперечать міжнародним стандартам у сфері свободи слова, доступу до інформації та захисту прав людини. Проте завдяки використанню риторики «національної безпеки» або «цифрового суверенітету» держави-автократії прагнуть виправдати свої дії на міжнародній арені, зокрема, в межах ООН, ОБСЄ та інших організацій.

Соціальні мережі у цифрову епоху стали не лише інструментом комунікації, а й потужним засобом формування громадської думки, мобілізації суспільства і навіть зміни політичних режимів. У зв'язку з цим держави, що прагнуть утвердити інформаційну автократію, зосередили особливу увагу на контролі над цифровими платформами.

Одним із базових механізмів контролю є вимога обов'язкової реєстрації або ліцензування діяльності соціальних мереж на території певної країни. Це дозволяє державним органам встановлювати локальні представництва компаній, які підпорядковуються національному законодавству і змушені виконувати вимоги щодо блокування контенту або передачі даних про користувачів.

Ще одним інструментом є законодавче встановлення обов'язків для платформ щодо модерації контенту. Соціальні мережі зобов'язуються оперативно видаляти інформацію, яка визнається незаконною або небажаною відповідно до національних актів. Деякі країни запроваджують так звані «локалізаційні закони», які вимагають зберігати дані громадян на території держави. Це спрощує доступ влади до особистої інформації користувачів без необхідності дотримання складних міжнародних процедур захисту персональних даних. Під виглядом забезпечення «цифрового суверенітету» фактично створюється механізм тотального нагляду.

Важливо звернути увагу й на створення спеціальних органів чи комісій із нагляду за діяльністю соціальних мереж. Такі органи часто отримують широкі повноваження: від видачі рекомендацій щодо блокування контенту до накладення штрафів або повного обмеження доступу до певних платформ. Їхня діяльність нерідко не супроводжується належними процедурами незалежного судового контролю, що суперечить принципам справедливого правосуддя та захисту прав людини. Отже державний контроль над соціальними мережами в умовах інформаційної автократії базується на законодавчих інструментах, які формально спрямовані на захист суспільних інтересів, але фактично використовуються для обмеження свободи слова, права на приватність та громадянської активності.

В умовах інформаційної автократії постає фундаментальне протиріччя між прагненням держави регулювати цифровий простір і зобов'язанням поважати права людини та забезпечувати свободу вираження поглядів. Застосування цензури щодо контенту в соціальних мережах нерідко порушує принцип рівності доступу до інформації. Контрольований державою фільтр дозволяє штучно просувати одну групу наративів та маргіналізувати інші, що веде до фактичного монополізму у сфері інформаційного обміну. Це суперечить етичному принципу плюралізму думок, який є наріжним каменем демократичного суспільства. Існує серйозна етична дилема щодо захисту приватності користувачів. Законодавчі вимоги щодо локалізації даних та їх відкриття за запитом держави позбавляють громадян реального контролю над своєю особистою інформацією. Відсутність прозорості у процедурах доступу до персональних даних створює небезпеку масового стеження і репресій проти політично активних осіб. Під тиском держави приватні компанії – власники соціальних мереж – змушені ставати учасниками процесу цензурування і контролю.

Це породжує нові етичні виклики: чи можуть приватні корпорації, що декларують прихильність до прав людини, виконувати вимоги, які очевидно порушують ці права? Як забезпечити відповідальність таких компаній перед громадськістю?

Правові дилеми також стосуються питання судового захисту прав користувачів. У багатьох юрисдикціях громадяни позбавлені ефективних механізмів оскарження рішень про блокування акаунтів, видалення контенту чи передачу їхніх даних державним органам. Це ставить під сумнів дотримання базових стандартів справедливого процесу і верховенства права у цифровому середовищі.

Важливо зазначити, що міжнародні організації (зокрема, ООН, Рада Європи [4]) неодноразово наголошували: будь-які обмеження свободи вираження у цифровій сфері повинні бути чітко обґрунтовані, пропорційні та підлягати незалежному судовому контролю. В умовах інформаційної автократії ці принципи ігноруються, що свідчить про системну кризу права в цифровому просторі. Державний контроль над соціальними мережами у режимах інформаційної автократії створює глибокі правові та етичні виклики. Він ставить під загрозу фундаментальні права людини, руйнує довіру до цифрового середовища та сприяє поступовій деградації принципів демократії, свободи і правової держави у глобальному масштабі.

Висновки. У результаті проведеного теоретико-правового аналізу можна зробити низку концептуальних висновків щодо природи, структури та впливу законодавчих механізмів інформаційного контролю в умовах інформаційної автократії.

Інформаційна автократія є еволюційною формою авторитарного режиму, що функціонує не лише шляхом грубого насильства чи прямої цензури, а через складну систему юридично оформлених норм. Законодавство тут виступає не гарантом прав і свобод, як у демократичних правопорядках, а навпаки – засобом їх обмеження. Саме на рівні законодавчих актів відбувається легітимація авторитарного контролю за інформаційним простором. Правова оболонка таких механізмів дозволяє владі створювати ілюзію відповідності правовим стандартам, що особливо актуально у зовнішньополітичному контексті, коли держави-автократії апелюють до «захисту національних інтересів» та «інформаційного суверенітету».

Законодавчі механізми контролю над інформаційним простором в інформаційних автократіях мають системний характер і не є ізольованими. Вони охоплюють різні рівні регулювання: від обмеження доступу до інформації через вимоги до ліцензування медіа і платформ, до контролю за поширенням (регламентація змісту, блокування контенту) і споживанням інформації (моніторинг активності користувачів, обов'язкова ідентифікація, зберігання даних тощо). Така багаторівнева структура забезпечує високий ступінь проникнення державного контролю у всі фази інформаційної взаємодії.

Важливим інструментом є прийняття законів із невизначеним, оціночним або розмитим змістом. Поняття на кшталт «небажана інформація», «образа держави», «підлив національної безпеки» чи «фейки» залишають значний простір для дискреції з боку державних органів. Це відкриває можливості для вибіркового правозастосування та політично вмотивованих репресій. Таким чином, юридична невизначеність використовується як інструмент тиску на опозицію, громадянське суспільство та незалежні медіа.

Аналіз прикладів з практики окремих держав (Китай, Росія, Туреччина, Іран, Індія) засвідчує, що законодавчі механізми інформаційного контролю здебільшого комбінуються з технічними засобами, зокрема: DPI, автоматичними системами блокування, інструментами стеження за онлайн-активністю, вимогами до локалізації даних тощо. Це створює «цифрову автократію», в якій поєднуються формально легальні механізми та технологічні інструменти примусу й стеження.

Особливу загрозу становить тенденція до делегування державного контролю приватним цифровим платформам, які юридично зобов'язуються самостійно фільтрувати контент, надавати дані користувачів та співпрацювати з владою. Це створює ситуацію, коли цензура відбувається в обхід офіційної процедури, що ускладнює фіксацію правопорушень і позбавляє користувачів ефективних механізмів захисту.

Законодавчі механізми інформаційного контролю прямо суперечать основоположним міжнародним актам у сфері захисту прав людини. І хоча держави-автократії використовують риторику безпеки, на практиці такі дії підривають універсальні цінності свободи слова, права на приватність та плюралізм думок.

Законодавчі механізми контролю в інформаційних автократіях є елементами гібридної правової системи, в якій демократична форма (закони, суди, норми) поєднується з авторитарним змістом (примус, ідеологічний контроль, придушення свободи). Їх небезпека полягає не лише у поточному обмеженні прав, а й у трансформації правового мислення, коли громадяни поступово звикають до того, що обмеження свободи слова є нормою, а не відхиленням. У цьому контексті постає завдання подальшого дослідження юридичних, політичних і філософських передумов для забезпечення стійкого інформаційного балансу в цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Stanford University. *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. URL: <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017>.
2. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. URL: <https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf>.
3. WIPO lex. *İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun*. URL: <https://wipolex-resources-eu-central-1-358922420655.s3.amazonaws.com/edocs/lexdocs/laws/tr/tr101tr.pdf>.
4. Рекомендація CM/Rec(2018) 2 Комітету Міністрів державам-членам про ролі та обов'язки Інтернет-посередників від 07.03.2018. URL: https://thedigital.gov.ua/storage/uploads/files/normative_document/archive/5bcf04496e848695859521.pdf.
5. Freedom House (2023). *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence*. URL: <https://freedomhouse.org/report/freedom-net/2023/repressive-power-artificial-intelligence>.