



# **ПРОТИДІЯ ДЕЗІНФОРМАЦІЇ В ІНТЕРНЕТІ: КУДИ РУХАТИСЯ УКРАЇНІ?**

**ГРУДЕНЬ 2021**

## **АВТОРИ:**

**Максим Дворовий** - Лабораторія цифрової безпеки, юрист

**Анна Людв**а - Лабораторія цифрової безпеки,  
молодша юристка

**ЛАБОРАТОРІЯ ЦИФРОВОЇ БЕЗПЕКИ** — громадська організація, що працює над створенням сприятливого середовища для реалізації цифрових прав людини через проведення аналізу та розробку рекомендацій щодо державної політики у сфері інтернет свобод та врядування, а також надає підтримку з цифрової безпеки правозахисникам, журналістам, медійним та іншим організаціям громадянського суспільства в Україні та Східній Європі.

## **Аналітичний звіт підготовлено за підтримки Американської Асоціації Юристів Ініціативи з Верховенства Права (ABA ROLI) в Україні.**

Матеріали, що містяться у цьому документі, відображають думки авторів та редакторів і не повинні тлумачитися як такі, що відображають офіційну позицію Американської Асоціації Юристів. Інформація, яка міститься в цьому документі, не повинна розглядатися як надання юридичних консультацій у конкретних випадках, і читачі несуть відповідальність за отримання таких консультацій від своїх юристів. Цей матеріал призначений винятково для освітніх та/або інформаційних цілей.

## ЗМІСТ

Дезінформація: труднощі визначення? .....	4
Пеналізація та блокування дезінформації в інтернеті у світі: наскільки вони відповідають міжнародним стандартам у сфері свободи вираження поглядів? .....	6
Чи можна змусити соцмережі обмежувати дезінформацію? .....	11
Інституційний вимір протидії дезінформації .....	14
Поширення дезінформації та Україна: спроби законодавчої протидії .....	16
Пандемія Covid-19: чи була Україна готовою до інфодемії? .....	19
Українські інституції для протидії дезінформації .....	22
Висновки та рекомендації .....	27

## Дезінформація: труднощі визначення?

Дезінформація відносно нещодавно стала об'єктом прицільних юридичних досліджень. Проблема, пов'язана з завданням шкоди від її поширення, актуалізувалася в цифровому світі та призвела до різкого збільшення активності держав та міжнародних організацій у сфері протидії цьому явищу. Почалися дискусії щодо термінології і предмета боротьби з дезінформацією. Від цієї термінологічної дискусії залежать і заходи, які держави повинні впроваджувати, аби боротися з фейками. Втім, станом на 2021 рік єдиного та вичерпного визначення поняття дезінформації сформульовано не було, що спонукає національні уряди, які намагаються протидіяти її поширенню, до власних інтерпретацій.

Першим орієнтиром на міжнародній арені стала Спільна декларація спеціальних доповідачів з питань свободи вираження поглядів міжнародних організацій щодо свободи вираження поглядів, «фейкових новин», дезінформації та пропаганди у 2017 році.<sup>1</sup> Вона визначила дезінформацію як «висловлювання, що є очевидно неправдивими, або щодо яких можна розумно очікувати, що вони є неправдивими». Клер Уордл та Хосейн Дарахшан у своєму дослідженні для Ради Європи описують три види інформації, яка може схарактеризувати фейки:

- дезінформація (disinformation) – неправдива та свідомо створена для заподіяння шкоди людині, соціальній групі, організації чи країні інформація;
- неправдива інформація (misinformation) – помилкова, але створена без наміру завдати шкоди, інформація;
- спотворена інформація (malinformation) – інформація, що ґрунтується на реальних фактах, використовується для заподіяння шкоди особі, організації або країні.<sup>2</sup>

Кодекс ЄС з протидії дезінформації, який у 2018 році підписали найбільші технологічні компанії, аби скооперуватися у протидії цьому шкідливому явищу, визначає дезінформацію як підтверджено хибну чи оманливу інформацію, що створюється, подається та поширюється з метою економічної вигоди або навмисного введення громадськості в оману, та може завдати суспільної шкоди, як-от загроза демократичним політичним процесам та процесам розроблення політик, захисту здоров'я громадян ЄС, довкілля або безпеки.

<sup>1</sup> OSCE Representative on Freedom of the Media, Joint declaration on freedom of expression and “fake news”, disinformation and propaganda (3 March 2017): <https://www.osce.org/files/f/documents/6/8/302796.pdf>

<sup>2</sup> Claire Wardle, Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008): <https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>

Це визначення і надалі використовується у більшості документів ЄС, що стосуються протидії цьому явищу. Окремо наголошується, що до дезінформації не відносяться оманлива реклама, помилки у висвітленні новин, сатира, пародія та чітко ідентифіковані партійні новини чи коментарі.<sup>3</sup>

У 2021 році свій звіт на тему «Дезінформація та свобода думки і вираження поглядів» видала спеціальна доповідачка ООН з промоції та захисту свободи думки і вираження поглядів Ірен Хан. Вона пропонує визначати дезінформацію як неправдиву інформацію, що розповсюджується з наміром спричинити серйозну соціальну шкоду, а неправдиву інформацію (misinformation) як неусвідомлене поширення помилкової інформації.<sup>4</sup>

В усіх звітах, згаданих вище, увага концентрується саме на боротьбі з поширенням дезінформації як явища, з меншим акцентом на протидії поширенню неправдивої інформації. Саме тому в цьому матеріалі ми також сконцентруємося на аналізі того, як держави намагаються протидіяти дезінформації. Дезінформацію ми розглядатимемо через призму таких ознак:

- усвідомлена та така, що може бути підтверджена, недостовірність інформації, що поширюється;
- поширення задля економічної вигоди або навмисного обману аудиторії;
- намір та можливість зашкодити публічному інтересу при її поширенні.

Варто пам'ятати, що дезінформація в інтернеті може поширюватися різноманітними способами. Приміром, реклама, що таргетується на дуже вузьку категорію осіб та здатна розпалювати протистояння у суспільстві; неправдива новина, що поширюється за допомогою ботів, фейкових акаунтів знаменитостей; накручування рейтингів контенту шляхом реагування на нього. Це може бути посилення з неперевіреною інформацією, що необдуманно поширюється звичайним користувачем, або ж умисно з певним наміром розповсюджується відомою людиною. Всі ці типи поширення інформації вимагають різної протидії зі сторони держави та приватних компаній відповідно до міжнародних стандартів дотримання прав людини.

---

<sup>3</sup> EU Code of Practice on Disinformation:  
<https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

<sup>4</sup> 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, Irene Khan (2021):  
<https://undocs.org/A/HRC/47/25>

## Пеналізація та блокування дезінформації в інтернеті у світі: наскільки вони відповідають міжнародним стандартам у сфері свободи вираження поглядів?

Зі збільшенням усвідомлення загроз, пов'язаних з поширенням дезінформації, держави почали шукати шляхи протидії цьому явищу. Як це трапляється найчастіше, першим заходом з протидії, який спадає на думку можновладцям, є заборона поширення певного типу контенту або ж його блокування. Такі заходи проблемні з багатьох підстав: держави створюють надзвичайно широкі формулювання для відповідних положень законодавства, передбачають надмірні санкції і свавільно застосовують їх для того, аби приглушити критиків уряду або ж керівного режиму, а також не забезпечують належної процедури розгляду відповідних питань у судових чи інших незалежних органах.

Нагадаємо, що будь-які обмеження свободи вираження поглядів, відповідно до статті 19 Міжнародного пакту про громадянські та політичні права (а у європейському контексті – ще і статті 10 Європейської конвенції про права людини) мають відповідати трискладовому тесту, а саме:

- передбачатися законом;
- мати легітимну мету;
- бути необхідними та пропорційними.<sup>5</sup>

Міжнародні організації у сфері захисту прав людини не надто прихильно ставляться до заходів із заборони чи блокування дезінформації як типу контенту. У вже згаданій Спільній декларації спеціальні доповідачі наголошують, що будь-які загальні заборони на поширення інформації, що базуються на розмитих концепціях на кшталт **«неправдивих новин»** або **«необ'єктивної інформації»** суперечать міжнародним стандартам обмеження свободи вираження поглядів.<sup>6</sup> Спеціальна доповідачка ООН Ірен Хан підкреслила, що більшість таких законів нечітко визначають поняття неправдивої інформації (зокрема, застосовуючи для визначень кругову логіку на кшталт «висловлювання є неправдивим, якщо воно є неправдивим або оманливим») та не вимагають встановлення сильного й належного зв'язку між спричиненою шкодою та вчиненим діянням.<sup>7</sup> Водночас вона припускає можливість встановлення заборони на поширення дезінформації у вузько визначених сферах та з урахуванням таких вимог: між висловлюванням та завданою шкодою

<sup>5</sup> Міжнародний пакт про громадянські та політичні права:  
[https://zakon.rada.gov.ua/laws/show/995\\_043](https://zakon.rada.gov.ua/laws/show/995_043)

<sup>6</sup> OSCE Representative on Freedom of the Media, Joint declaration on freedom of expression and “fake news”, disinformation and propaganda (3 March 2017)  
<https://www.osce.org/files/f/documents/6/8/302796.pdf>

<sup>7</sup> 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, Irene Khan (2021):  
<https://undocs.org/A/HRC/47/25>

має бути прямий причинно-наслідковий зв'язок, а заборона має враховувати тяжкість та негайність настання шкоди.

Європейський суд з прав людини свого часу наголошував, що **«стаття 10 Конвенції не забороняє обговорення або поширення отриманої інформації, навіть якщо виникають серйозні сумніви щодо її достовірності; якби це було не так, то це ... накладало б необґрунтовані обмеження на свободу вираження поглядів, гарантовану статтею 10 Конвенції»**.<sup>8</sup> Суд ECOWAS<sup>9</sup> та Східноафриканський суд справедливості<sup>10</sup> стверджували, що **«практика накладення кримінальних санкцій щодо ... поширення неправдивих новин має наслідком охолоджувальний ефект, що може неналежно обмежити право на свободу вираження поглядів журналістів»**.

Щодо блокувань сайтів позиція в міжнародному праві є чіткішою: блокування сайтів, IP-адрес, портів, мережевих протоколів та окремих сервісів (як-от соціальні мережі) є надзвичайним заходом, який може бути виправданий лише відповідно до міжнародних стандартів – тобто повинен передбачатися законом, мати легітимну мету, бути пропорційним, застосовуватися лише у випадку неможливості застосування менш обмежувальних заходів та за дотримання гарантій належного процесу.<sup>11</sup>

Тренд криміналізації поширення дезінформації та блокування ресурсів, що її поширюють, не є локалізованим, а приклади такого законодавства можна зустріти на різних континентах.<sup>12</sup> У багатьох випадках каталізатором до прийняття відповідного законодавства стала пандемія Covid-19. Вірменія, наприклад, пішла шляхом відступу від зобов'язань за Європейською конвенцією з прав людини і у відповідній заяві зазначила, що будь-яка інформація про коронавірус, зокрема про кількість хворих, стан їхнього здоров'я, кількість проведених тестів, може публікуватися винятково як посилання на офіційну інформацію, а будь-яку інформацію, що не відповідає офіційній, особи,

---

<sup>8</sup> Salov v Ukraine App no 65518/01 (ECtHR, 6 September 2005): <http://hudoc.echr.coe.int/eng?i=001-70096>

<sup>9</sup> Federation of African Journalists and Others v The Gambia App no 36/15 (ECOWAS Court, 13 February 2018): <https://ihrda.uwazi.io/en/document/w9z5b6xfwy?page=47>

<sup>10</sup> Media Council of Tanzania and 2 Others v The Attorney General of the United Republic of Tanzania No 2/2017 (EACJ, 28 March 2019): <https://www.eacj.org/?cases=reference-no-2-of-2017-media-council-of-tanzania-legal-and-human-rights-centre-tanzania-human-rights-defenders-coalition-vs-the-attorney-general-of-the-united-republic-of-tanzania>

<sup>11</sup> OSCE Representative on Freedom of the Media, Joint declaration on freedom of expression and “fake news”, disinformation and propaganda (3 March 2017): <https://www.osce.org/files/f/documents/6/8/302796.pdf>

<sup>12</sup> Poynter, A guide to anti-misinformation actions around the world: <https://www.poynter.org/ifcn/anti-misinformation-actions/>

що її поширили, повинні негайно видаляти.<sup>13</sup>

Серед країн-членів Ради Європи можна також згадати законодавство Угорщини, де було впроваджено відповідальність за поширення дезінформації під час пандемії у розмірі до 5 років ув'язнення.<sup>14</sup> У Росії на доповнення норм, що вже існували, ввели адміністративну відповідальність за **«публічне поширення завідомо недостовірної інформації під виглядом достовірних повідомлень про обставини, що можуть становити загрозу життю і здоров'ю громадян»** про пандемію з кількомільйонними штрафами в рублях для порушників, а також кримінальну відповідальність у разі, якщо поширення фейків призведе до тяжких наслідків для здоров'я людини або її смерті, з потенційним ув'язненням до 5 років.<sup>15</sup> Ще до пандемії там також була передбачена можливість блокувати сайти, які поширюють недостовірну інформацію, що може зашкодити життю та здоров'ю громадян, загрожувати масовими порушеннями публічного порядку чи призупиненню функціонування життєво важливої інфраструктури.<sup>16</sup>

Також ще до пандемії до свого медійного законодавства поправки внесла і Білорусь. Відповідно до них медіа заборонили поширювати недостовірну інформацію, що може завдати шкоди державним чи публічним інтересам. Наслідками такого поширення стане застосування адміністративної відповідальності.<sup>17</sup> Всі згадані акти піддавалися суттєвій критиці, адже з огляду на авторитарні тенденції керівників цих держав, існувала значна загроза застосування законодавства для придушення свободи слова, попри позірну відповідність термінології міжнародним визначенням дезінформації та потребу встановлювати причинно-наслідковий зв'язок між поширенням інформації та шкідливими наслідками визначеним інтересам (хоча подекуди, як у Білорусі, де законодавець обмежився формулюванням “державний чи публічний інтерес” без його деталізації, сам перелік цих інтересів залишав бажати кращого).

---

<sup>13</sup> Derogation of Armenia from the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No 005):

<https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=005&codeNature=0>

<sup>14</sup> Shaun Walker, “Hungarian journalists fear coronavirus law may be used to jail them” The Guardian (Budapest, 3 April 2020):

<https://www.theguardian.com/world/2020/apr/03/hungarian-journalists-fear-coronavirus-law-may-be-used-to-jail-them>

<sup>15</sup> Государственная дума Федерального Собрания Российской Федерации, “Парламентом приняты законы по противодействию коронавирусу”:

<http://duma.gov.ru/news/48196/>

<sup>16</sup> Федеральный закон О внесении изменений в статью 15.3 Федерального закона “Об информации, информационных технологиях и о защите информации” от 18.03.2019 N 31-ФЗ:

[http://www.consultant.ru/document/cons\\_doc\\_LAW\\_320401/](http://www.consultant.ru/document/cons_doc_LAW_320401/)

<sup>17</sup> Янина Воронко, «Fake news: как страны борются с недостоверными новостями» (ilex.by):

<https://ilex.by/news/fake-news-kak-strany-boryutsya-s-nedostovernymi-novostyami/>



Франція пішла іншим шляхом, точково сконцентрувавши свої зусилля на протидії маніпуляціям у передвиборчий період. Саме тоді французькі суди можуть за пришвидшеною процедурою обмежувати доступ до фейків, оширених умисно та у великих кількостях з метою вплинути на вибори. Втім, законодавство не покладає індивідуальної кримінальної чи адміністративної відповідальності на поширювачів дезінформації, обмежуючись судовими обмеженнями на поширення такої інформації та також концентрується на встановленні зобов'язань з прозорості щодо витрат на політичну рекламу та з запровадження механізмів скарг на контент до великих інтернет-платформ.<sup>18</sup> Нагляд за дотриманням інтернет-платформами вимог щодо опублікування власних заходів з протидії фейкам здійснює Вища аудіовізуальна рада Франції. Вона ж опублікувала рекомендації щодо обов'язку співпраці у протидії дезінформації та окрім вимог до механізмів оскарження протиправного контенту також закликала компанії оприлюднити власні алгоритми і боротися з акаунтами, що масово поширюють дезінформацію.<sup>19</sup>

Німецьке законодавство, хоч прямо і не стосується поширення дезінформації та її криміналізації (найближчим до дезінформації типом протиправного контенту, на який діє акт, є дифамація та образа), покладає на соцмережі, кількість користувачів яких у Німеччині перевищує 2 мільйони, обов'язок один раз на пів року звітувати про отримані скарги на розповсюдження на їхніх платформах протиправного контенту. Такі соцмережі також мають запровадити на платформах ефективну та прозору систему розгляду скарг на контент і видаляти його протягом 24 годин (для очевидно протиправного контенту) або 7 днів (для “простого” протиправного контенту) після отримання скарги. Штрафи за порушення цих вимог можуть досягати 5 мільйонів євро.<sup>20</sup> Попри первісні побоювання представників громадянського суспільства щодо того, що NetzDG може серйозно вплинути на свободу слова в соцмережах, він не призвів до суттєвого зростання масиву видаленого контенту чи накладення на соцмережі значних штрафів<sup>21</sup>, поліпшивши прозорість інтернет-гігантів.<sup>22</sup>

<sup>18</sup> French Government, Against information manipulation:  
<https://www.gouvernement.fr/en/against-information-manipulation>

<sup>19</sup> Recommandation n° 2019-03 du 15 mai 2019 du Conseil supérieur de l'audiovisuel aux opérateurs de plateforme en ligne dans le cadre du devoir de coopération en matière de lutte contre la diffusion de fausses informations: <https://www.csa.fr/Reguler/Espace-juridique/Les-textes-reglementaires-du-CSA/Les-deliberations-et-recommandations-du-CSA/Recommandations-et-deliberations-du-CSA-relatives-a-d-autre-s-sujets/Recommandation-n-2019-03-du-15-mai-2019-du-Conseil-superieur-de-l-audiovisuel-aux-operateurs-de-plateforme-en-ligne-dans-le-cadre-du-devoir-de-cooperation-en-matiere-de-lutte-contre-la-diffusion-d-e-fausses-informations>

<sup>20</sup> Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act):  
[https://www.bmjbv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG\\_engl.pdf](https://www.bmjbv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf)

<sup>21</sup> ICYMI, «New Report on Germany's NetzDG Online Hate Speech Law Shows No Threat of Over-Blocking» (27 November 2018): <https://www.counterextremism.com/press/icymi-new-report-germany%E2%80%99s-netzdg-online-hate-speech-law-shows-no-threat-over-blocking>

<sup>22</sup> Google, «Видалення контенту відповідно до закону Німеччини “Про захист прав користувачів у соціальних мережах”»: <https://transparencyreport.google.com/netzdg/youtube>

Втім, ідеї, закладені в цей акт, негативно вплинули на розвиток регулювання протидії дезінформації в авторитарних режимах.<sup>23</sup>

Перемістимося до Південно-Східної Азії, яка є одним зі світових центрів пеналізації поширення дезінформації. Наприкінці 2019 року в Сингапурі прийняли Protection from Online Falsehoods and Manipulation Act.<sup>24</sup> Він забороняє поширювати неправдиві твердження про факти, якщо вони загрожують національній безпеці, публічному здоров'ю чи спокою, можуть погіршити стосунки Сингапуру з іншими державами, впливають на вибори, здатні розпалити ворожнечу або підірвати суспільну довіру в виконання державними органами власних обов'язків. За поширення цієї інформації порушнику міг загрожувати штраф у розмірі до 50 000 сингапурських доларів (приблизно 37 000 доларів США) або ж ув'язнення на строк до 5 років. Він також передбачає можливість місцевого органу влади, відповідального за медіа та комунікації, за вказівкою міністра застосувати до посередників низку судових наказів для обмеження доступу до відповідного контенту або, у виняткових випадках, до ресурсу, що його поширює.

У Малайзії схоже законодавство було прийняте у 2018 році, скасоване у 2019, і потім знову запроваджене на тлі пандемії як указ короля Малайзії.<sup>25</sup> Цей указ стосується неправдивої інформації про Covid-19 та введеного у зв'язку з пандемією надзвичайного стану. За публікацію інформації з наміром розпалити страх у суспільстві порушнику може загрожувати до 3 років позбавлення волі. Указ передбачає необхідність обмеження доступу до протиправного контенту за зверненням поліції чи уповноваженого органу. Подібні заходи впроваджувалися і в інших державах регіону – Таїланді, Камбоджі та В'єтнамі.<sup>26</sup>

Африка не стала винятком. У Кенії у 2017 році було криміналізовано умисну публікацію неправдивих даних з наміром подати їх як правдиві, покарання порушника – 2 роки позбавлення волі або значний штраф.<sup>27</sup> Алжир у 2020 році додав до свого кримінального законодавства статтю, що передбачала відповідальність за публічне поширення неправдивої інформації, яка може

---

<sup>23</sup> Jacob Mchangama and Joelle Fiss, The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship (Justitia, November 2019): [http://justitia-int.org/wp-content/uploads/2019/11/Analyse\\_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf](http://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf)

<sup>24</sup> Protection from Online Falsehoods and Manipulation Bill (Bill No 10/2019): <https://sso.agc.gov.sg/Bills-Supp/10-2019>

<sup>25</sup> Emergency (Essential Powers) (No 2) Ordinance 2021: [https://drive.google.com/file/d/1ZOWsLPsqNL-fulcS3w7LRsmYnqeRWk\\_/view](https://drive.google.com/file/d/1ZOWsLPsqNL-fulcS3w7LRsmYnqeRWk_/view)

<sup>26</sup> Ralph Jennings, «In the name of “fake news” Asian governments tighten control on social media» (LA Times, 8 February 2019): <https://www.latimes.com/world/asia/la-fg-asia-fake-news-20190130-story.html>

<sup>27</sup> The Computer and Cybercrimes Bill 2017: [http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/ComputerandCybercrimesBill\\_2017.pdf](http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2017/ComputerandCybercrimesBill_2017.pdf)

підважити публічну безпеку або порядок.<sup>28</sup>

Більшість таких норм тією чи іншою мірою надмірно втручаються у свободу вираження поглядів з різноманітних причин. Це може бути як нечітка дефініція, так і надмірна санкція, як позасудовий порядок обмеження доступу до інформації залежним адміністративним органом, так і відсутність вказівки на шкідливі наслідки поширення дезінформації. Але яким чином тоді протидіяти дезінформації, як не застосуванням санкцій за її поширення? Багато дослідників пропонує сфокусуватися на регулюванні соціальних мереж, зокрема на їхній прозорості.<sup>29</sup>

## Чи можна змусити соцмережі обмежувати дезінформацію?

Соціальні мережі та платформи стали чи не найнебезпечнішим середовищем для поширення дезінформації. Завдяки механізмам, які вони надають – створення дописів, розповсюдження гіперпосилань, пересилання повідомлень у великих групах тощо, поширення дезінформації ампліфікується. Крім того, в окремих сферах його важко регулювати, адже часто інформація поширюється у приватних чатах, де, теоретично, відстежування розповсюдження інформації має бути неможливим. Втім, відповідні платформи мають і публічний функціонал, на спробах регулювати який ми і сконцентруємося.

Нагадаємо, що в будь-якому разі соцмережі є інтернет-посередниками, що мають імунітет від відповідальності за контент, який на їхніх платформах поширюють користувачі. Цей імунітет може обмежуватися у випадках, коли соцмережа отримує відомості про протиправну діяльність та контент або про обставини, з яких випливає очевидно протиправний характер такої діяльності, та, отримавши відомості про таку діяльність та контент, не діє достатньо оперативно з метою припинення діяльності чи поширення контенту.<sup>30</sup> Подальші рекомендації Ради Європи у цій сфері наголошують, що видалення контенту за запитом держави має відбуватися лише на підставі судового наказу

<sup>28</sup> MENA Rights Group, Algeria: Penal code amendments restrict freedoms of expression and association: <https://www.menarights.org/en/articles/algeria-penal-code-amendments-restrict-freedoms-expression-and-association>

<sup>29</sup> Claire Wardle, Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making (2nd edn, CoE 2008):

<https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77>;

ICNL, Legal Responses to Disinformation: A Policy Prospectus:

<https://www.icnl.org/wp-content/uploads/2021.03-Disinformation-Policy-Prospectus-final.pdf>

<sup>30</sup> Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce):

<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN>

або акту іншого незалежного регулятора, за винятком випадків, що стосуються матеріалів, які містять сексуальну експлуатацію та насильство над дітьми, чи інших матеріалів, де обмеження доступу потребує швидших заходів.<sup>31</sup> З практики Європейського суду з прав людини можна дійти висновку, що таким контентом може бути мова ворожнечі<sup>32</sup>; питання щодо віднесення до цього контенту дезінформації залишається відкритим.

Спеціальна доповідка ООН з промоції та захисту свободи думки і вираження поглядів Ірен Хан у своєму звіті вказала, що:

- держави зобов'язані гарантувати, що компанії поважатимуть права людини – вони не повинні змушувати компанії видаляти або блокувати контент, що є легальним відповідно до міжнародного права захисту прав людини, і не вимагати від них визначати легальність контенту відповідно до національного законодавства замість судів, в той час, як компанії повинні бути прозорими щодо таких запитів держав і утримуватися від домовленостей з державами щодо видалення контенту за зачиненими дверима;
- державне регулювання соціальних медіа має бути зосереджене на забезпеченні прозорості належних правових процедур для користувачів, due diligence щодо прав людини з боку компаній, а також на забезпеченні того, щоб незалежність і повноваження регуляторів були чітко визначені, гарантовані та обмежені законом.<sup>33</sup>

Серед чільних ініціатив у цій сфері варто відзначити проєкт Акту про цифрові послуги (Digital Services Act, DSA), впровадження якого зараз активно обговорюється в рамках Європейського Союзу.<sup>34</sup> Він є логічним наслідком політики ЄС останніх років, яка була сконцентрована на закликах до технологічних компаній щодо збільшення прозорості їхніх внутрішніх процесів, пов'язаних з поширенням інформації. У ньому також можна побачити відлуння французького та німецького підходів, описаних вище. У разі прийняття DSA стане орієнтиром для світу щодо регулювання соцмереж та поширення дезінформації на їхніх платформах.

---

<sup>31</sup> Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries:  
<https://rm.coe.int/1680790e14>

<sup>32</sup> Delfi AS v Estonia [GC] App no 64569/09 (ECtHR, 16 June 2015)  
<http://hudoc.echr.coe.int/eng?i=001-155105>

<sup>33</sup> 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, Irene Khan (2021):  
<https://undocs.org/A/HRC/47/25>

<sup>34</sup> Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC:  
<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0825&from=en>

DSA не визначає конкретні категорії протиправного контенту, але в окремих положеннях преамбули розрізняє цю категорію та категорію «дезінформація». Щодо протиправного контенту, то проєкт DSA передбачає впровадження на національному рівні судових наказів щодо вчинення дій проти контенту, де мають бути зазначені причини протиправності та URL контенту, його територіальний обсяг, та має вказуватися перелік дій, які повинні вчинити посередники щодо такого контенту. Кожен інтернет-посередник муситиме забезпечити наявність єдиної контактної особи для прямої комунікації щодо впровадження DSA. У разі, якщо компанія зареєстрована за межами Європейського Союзу, то вона має визначити фізичну чи юридичну особу, що представлятиме її інтереси у ЄС в одній з держав, де посередник надає свої послуги, з метою дотримання обов'язків за DSA.

До всіх інтернет-посередників застосовуватиметься обов'язок передбачити у своїх правилах користування обмеження, пов'язані з використанням сервісу, що мають бути зрозумілими та публічно доступними, а також оприлюднювати інформацію про модерацію контенту, зокрема отримані запити на його видалення. Це має слугувати прозорості інтернет-посередників перед користувачами та надати їм розуміння того, як насправді діятимуть правила користування тим чи іншим сервісом на практиці.

Онлайн-платформи муситимуть розробити внутрішні системи розгляду скарг. Протягом 6 місяців з моменту винесення рішення про обмеження доступу до інформації, припинення надання певної послуги чи обмеження доступу до акаунта відповідно до правил користування послугою, користувачі повинні отримати можливість безкоштовного перегляду рішення в електронній формі. Ці системи мають бути доступними, дружніми до користувачів та допомагати створювати належно обґрунтовані скарги. Користувачі також мають отримати доступ до позасудових засобів розгляду власних скарг: ці положення слугують забезпеченню права користувачів до ефективних засобів правового захисту у відносинах з потужнішими онлайн-платформами. До дуже великих онлайн-платформ, сервісами яких в ЄС щомісячно користується понад 45 мільйонів осіб, висувається ще більший обсяг обов'язків, зокрема щодо оцінки ризиків правам людини у власній діяльності та прозорості реклами.

DSA також створює інститут координаторів цифрових сервісів – національних регуляторів, що відповідатимуть за впровадження положень акта на національному рівні. Регулятори мають виконувати свої повноваження безсторонньо, належно та оперативно, а також мати достатню кількість ресурсів, аби ефективно працювати. Такі координатори отримуватимуть право накладати штрафи на посередників, що перебуватимуть під їхньою юрисдикцією, за порушення вимог DSA. Санкції не мають перевищувати 6 % річного обороту відповідного інтернет-посередника. Єврокомісія також отримає можливість притягувати посередників та онлайн-платформи до відповідальності на рівні Європейського Союзу.

У проєкті DSA творці акта напряду згадують дезінформацію у контексті кодексів поведінки, які вони розглядають як механізм співрегулювання та як системний ризик, що може виникнути під час діяльності онлайн-платформ. У цих кодексах поведінки повинні передбачатися правила, якими онлайн-платформи мають керуватися для зменшення ризиків у власній діяльності, а також порядок звітування щодо досягнення цілей, передбачених відповідними кодексами поведінки. Відмова запрошеної платформи в участі у такій схемі співрегулювання має враховуватися Єврокомісією при розгляді питання про порушення платформою обов'язків, передбачених DSA.

Подібний кодекс поведінки – Кодекс ЄС щодо протидії дезінформації – вже існує з 2018 року та має стати основою для співрегулювального акта після прийняття DSA.<sup>35</sup> Наразі він містить зобов'язання підписантів із забезпечення прозорості політичної та тематичної реклами, збільшення активності щодо закриття фейкових акаунтів, протидії ботам та пріоритизації достовірної інформації у новинній стрічці. Перший річний моніторинг дотримання положень Кодексу вказав на його загальну ефективність, втім наголосив на потребі розроблення чіткіших дефініцій у таких сферах, як тематична реклама, неавтентична поведінка тощо, а також необхідності охопити низку інших сфер, як-от мікротаргетинг чи накручування популярності певного типу контенту.<sup>36</sup>

Така співрегулювальна схема справді може бути ефективною, якщо для відповідної компанії важливий ринок, на якому вона оперує, або ж співрегулювання є для неї вигідною альтернативою жорсткішому регулюванню. Тому впровадження цього шляху в українському контексті, який наразі взагалі не передбачає жодного контролю, потребує значної роботи зі створення належного регуляторного фундаменту.

## Інституційний вимір протидії дезінформації

З огляду на заходи, застосовані в Україні на сьогодні, ми зупинимося на іншому вимірі – інституційному. Саме інституції з розвитку стратегічних комунікацій<sup>37</sup> мають досліджувати дезінформацію та протидіяти їй шляхом спростування фейків та формування власних наративів. Одними з перших на важливість стратегічних комунікацій звернули увагу в НАТО. У квітні 2009 року, під час 60-го щорічного саміту, лідери НАТО вперше визнали доцільність та важливість

<sup>35</sup> EU Code of Practice on Disinformation:  
[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=54454](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=54454)

<sup>36</sup> EU Commission Staff Working Document, Assessment of the Code of Practice on Disinformation - Achievements and areas for further improvement (10 September 2020):  
[https://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=69212](https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69212)

<sup>37</sup> Congressional Research Service, NATO's 60th Anniversary Summit:  
<https://sgp.fas.org/crs/row/R40454.pdf>



стратегічних комунікацій. Зрештою, там було створено Центр досконалості стратегічних комунікацій НАТО (NATO Strategic Communications Centre of Excellence) – багатонаціональну міжнародну військову організацію, акредитовану НАТО.<sup>38</sup> Діяльність Центру об'єднує 14 країн, ще дві планували приєднатися до неї у 2021 році.

Стратком НАТО спрямовує свої зусилля на боротьбу з дезінформацією та запобігання поширенню фейкових новин. Варто підкреслити, що Стратком не здійснює щоденний моніторинг випадків дезінформації, натомість він займається підготовкою аналітичних звітів, покликаних виявляти шкідливі наративи, що розповсюджуються різноманітними гравцями, та підвищувати стійкість аудиторії до подібних наративів.<sup>39</sup> Цей орган займається стратегічною діяльністю на перетині інформаційної та медійної сфер, що дозволяє протидіяти глобальним акторам, що поширюють неправдиву інформацію, а не тактично усувати окремі елементи системи. Водночас його мінусом є робота винятково на захист альянсу, і дослідники стверджують, що діяльність Страткому не допомогла розвинути дієві системи інституційної протидії дезінформації на національному рівні держав-членів НАТО.<sup>40</sup>

Серйозною проблемою, яка потребувала створення відповідних інституцій, дезінформація стала і в рамках Європейського Союзу. Так, його система відповідних інституцій є більш розгалуженою, а їхня компетенція – ширшою. Передовсім, найвищу сходинку в системі органів посідає Європейська служба зовнішніх справ, що керує зовнішньою політикою, безпекою та обороною ЄС. У ній функціонує відділ стратегічних комунікацій та його оперативні групи.<sup>41</sup>

Однією з таких груп є East StratCom Task Force. Її основна функція полягає у розробленні комунікаційних продуктів та кампаній, що покликані краще роз'яснити цінності, інтереси та політику ЄС у країнах Східного партнерства. Як і Стратком НАТО, ця оперативна група займається аналізом загальних тенденцій щодо дезінформаційних наративів, що поширюються Кремлем. Вона також забезпечує функціонування інформаційного порталу EU vs Disinformation, що містить базу даних дезінформації, поширеної агентами Російської Федерації

---

<sup>38</sup> About NATO StratCom COE:  
[https://stratcomcoe.org/about\\_us/about-nato-stratcom-coe/5](https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5)

<sup>39</sup> CSIS, Countering Russian Disinformation (23 September 2020):  
<https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation>

<sup>40</sup> Kathleen J McInnis and Clementine G Starling, The Case for a Comprehensive Approach 2.0: How NATO Can Combat Chinese and Russian Political Warfare (Atlantic Council, June 2021):  
[https://www.atlanticcouncil.org/wp-content/uploads/2021/06/NATO-Comprehensive-Approach-Report-2021\\_final.pdf](https://www.atlanticcouncil.org/wp-content/uploads/2021/06/NATO-Comprehensive-Approach-Report-2021_final.pdf)

<sup>41</sup> EEAS, Strategic Communications:  
[https://eeas.europa.eu/headquarters/headquarters-homepage\\_en/100/Strategic%20Communications](https://eeas.europa.eu/headquarters/headquarters-homepage_en/100/Strategic%20Communications)

протягом останніх років.<sup>42</sup> Дещо відмінним від аналога в рамках НАТО є додатковий фокус на щоденній роботі та спростуванні окремих міфів чи наративів, розповсюджуваних медіа.

Окремо в рамках ЄС діє і Центр аналізу гібридних загроз у складі розвідувального та ситуаційного центру ЄС та Європейський Центр передового досвіду з протидії гібридним загрозам у Гельсінкі, Фінляндія. Їхні завдання охоплюють моніторинг та протидію гібридним загрозам з боку іноземних суб'єктів, які прагнуть вплинути на політичні рішення країн ЄС та його сусідів.<sup>43</sup>

Низка подібних центрів створюється і на національному рівні. Тут можна згадати Шведське управління психологічного захисту, що почне функціонувати з 2022 року і займатиметься психологічним захистом суспільства від дезінформації та підвищенням стійкості до зовнішніх інформаційних загроз.<sup>44</sup> Іншими прикладами є створений у Чеській Республіці Центр протидії тероризму та гібридним загрозам, якому доручено здійснювати моніторинг загроз і дезінформації, пов'язаних із внутрішньою безпекою, або підрозділи урядового зв'язку в державах Балтії, що відповідають за розвиток здатності державних комунікаційних структур реагувати на кризи безпеки, інформувати громадськість про шкідливу дезінформацію та сприяти зниженню її впливу в суспільстві.<sup>45</sup>

## **Поширення дезінформації та Україна: спроби законодавчої протидії**

Розглянувши міжнародні приклади законодавчого регулювання пеналізації та блокування дезінформації, варто сконцентруватися на українському досвіді законотворчості задля подолання викликів, що їх ставить поширення недостовірних фактів. Слід згадати, що наклеп як поширення завідомо неправдивих вигадок, які ганьблять особу, в Україні декриміналізовано ще з 2001 року.<sup>46</sup> Тому ця норма, на відміну від законодавства деяких інших країн, точно не могла б бути застосована для притягнення осіб до відповідальності.

<sup>42</sup> <https://euvsdisinfo.eu/>

<sup>43</sup> ABA ROLI, «Базовий документ з питань національної та кібербезпеки, інтернет-свободи та міжнародного права» (2020): <https://drive.google.com/file/d/18JoYJFZnL0I3mq04TCdzI96DYZetMlXT/view>

<sup>44</sup> MSB, Psykologiskt försvar: <https://www.msb.se/psykologisktforvar>

<sup>45</sup> ABA ROLI, «Базовий документ з питань національної та кібербезпеки, інтернет-свободи та міжнародного права» (2020): <https://drive.google.com/file/d/18JoYJFZnL0I3mq04TCdzI96DYZetMlXT/view>

<sup>46</sup> Кримінальний кодекс України (втратив чинність у 2001 році): <https://zakon.rada.gov.ua/laws/show/2001-05>



Водночас боротьба з дезінформацією стала однією з пріоритетних тем для уряду у 2019-2020 роках. Володимир Бородянський, що був міністром культури, молоді та спорту, стверджував про намір запровадити відповідну термінологію до національного законодавства.<sup>47</sup> Ці наміри втілилися у розроблення законопроекту про протидію дезінформації, презентованого в січні 2020 року.<sup>48</sup> Тоді ж цей законопроект<sup>49</sup> обговорили фахівці за участі представників уряду.

Які зміни пропонувалися Міністерством культури, молоді та спорту (МКМС)?

Перш за все, представники МКМС ініціювали ввести до законодавства термін «дезінформація». Дезінформацію пропонували визначати так: **«недостовірна інформація з питань, що становлять суспільний інтерес, зокрема стосовно національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, стану довкілля»**.<sup>50</sup> Передбачалося, що до дезінформації не можуть належати:

- оціночні судження, в тому числі критичні, за умови наявності мінімальної фактологічної основи;
- сатира та пародія, якщо під час розповсюдження чітко заявлено про сатиричний або пародійний характер розміщеної інформації;
- недобросовісна реклама.

Законопроект передбачав введення як адміністративної, так і кримінальної відповідальності за поширення недостовірної інформації. Зокрема штраф за розповсюдження дезінформації без добровільного її спростування становив 2000 розмірів мінімальної заробітної плати, що на момент дослідження дорівнювало 12 мільйонам гривень. До 600 000 гривень штрафу мали б заплатити в рамках цивільного провадження про спростування недостовірної інформації особи, що поширили її (за умови визнання інформації недостовірною).

До Кримінального кодексу України вводилася стаття 114-2, якою передбачався штраф до 170 000 гривень за систематичне (понад 3 рази протягом одного року) умисне масове розповсюдження завідомо недостовірних повідомлень про факти, події або явища, що становить загрозу національній безпеці, громадській безпеці, територіальній цілісності, суверенітету, обороноздатності України,

---

<sup>47</sup> <https://www.facebook.com/borodyanskiy/posts/10221753387210974>

<sup>48</sup> Детектор Медіа, «Презентація законопроекту про протидію дезінформації (СЛАЙДИ)» (17 січня 2020): <https://detector.media/infospace/article/173974/2020-01-17-prezentatsiya-zakonoproiektu-pro-protidyu-dezi-nformatsii-slaydy/>

<sup>49</sup> МКІП, «МКМС запрошує до обговорення проекту закону щодо забезпечення національної інфобезпеки та права на доступ до достовірної інформації» (20 січня 2020): <https://mkip.gov.ua/news/3343.html>

<sup>50</sup> Порівняльна таблиця законопроекту: [https://mkip.gov.ua/files/pdf/Disinformation\\_Draft\\_2020.pdf](https://mkip.gov.ua/files/pdf/Disinformation_Draft_2020.pdf)

права українського народу на самовизначення, життя та здоров'я громадян, стану довкілля протягом періоду відсутності повного контролю України за державним кордоном України. За використання для цього ботів або ж фінансування поширення дезінформації порушнику загрожує позбавлення волі строком до 5 років.

Окрім того, законопроект передбачав процедуру судового обмеження доступу до поширеної дезінформації у разі, якщо відповідь на заяву Уповноваженого з питань інформації не надається або ж якщо вона поширювалася без належних ідентифікаційних даних. Питання обмеження доступу до таких ресурсів мало б розв'язуватися за спеціальною процедурою в рамках адміністративного судочинства протягом 3 днів з моменту надходження заяви від Уповноваженого.

Хоча визначення, використані у проєкті, частково враховували дефініції, розроблені у Європейському Союзі, а норма Кримінального кодексу мала строковий характер дії (фактично, до припинення агресії) низка його положень суперечила міжнародно-правовим стандартам захисту прав людини. По-перше, запропоновані адміністративні санкції перевищували запропоновані кримінальні санкції, що не відповідає принципам встановлення відповідальності за діяння залежно від його суспільної небезпеки, а також створює загрозу застосування двох видів відповідальності до особи за одне діяння. Крім того, ці санкції були непропорційними. Поверталася й адміністративна відповідальність за дифамацію, що є неприпустимою в демократичному суспільстві. Окрім того, існував ризик притягнення до кримінальної відповідальності навіть якщо факти, які наводяться у публікації, є правдивими, але стосуються загроз, визначених законотворцем. Блокування дезінформації могло б відбуватися з формальних підстав та без належного аналізу матеріалів, що підпали б під блокування.<sup>51</sup>

Втім, цей законопроект не був реанімований після раундів обговорень. Також фактично стагнувала робота над проєктом Закону про медіа (№ 2693-д), яким передбачалося введення такої категорії забороненого для поширення в онлайн-медіа контенту як **«недостовірні матеріали щодо збройної агресії та діянь держави-агресора (держави-окупанта), її посадових осіб, осіб та організацій, що контролюються державою-агресором (державою-окупантом), у разі, якщо наслідком цього є розпалювання ворожнечі та ненависті або заклики до насильницької зміни, повалення конституційного ладу чи порушення територіальної цілісності чи конституційного ладу»**.<sup>52</sup> Заборона має діяти до моменту закінчення агресії. Попри те, що тут не фігурує термін «дезінформація», ця норма спрямована на заборону її поширення у контексті

<sup>51</sup> Віта Володовська, Людмила Опришко, Максим Дворовий, Олександр Бурмагін, «Юридичний аналіз законопроекту про дезінформацію» (Лабораторія цифрової безпеки, 23 січня 2020): <https://dslua.org/publications/yurydychnyy-analiz-zakonoproektu-pro-dezinformatsiiu/>

<sup>52</sup> Картка законопроекту: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=69353](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=69353)

агресії зі сторони Російської Федерації. Водночас цей термін фігурує у змінах до Виборчого кодексу України, що впроваджуються законопроектом, у контексті можливості Національної ради України з питань телебачення і радіомовлення укладати з платформами меморандуми про співпрацю у протидії дезінформації. Впровадження цієї норми є першою спробою в історії України нав'язати платформам м'яке співрегулювання. На жаль, перспективи прийняття цього закону є малоімовірними.

Призупинення процесів прийняття згаданих ініціатив не свідчить про однозначну відмову від планів впровадження законодавчого регулювання протидії дезінформації. 15 жовтня 2021 року Рада національної безпеки та оборони України затвердила Стратегію інформаційної безпеки України, яка наразі очікує підпису Президента України.<sup>53</sup> Позаяк її остаточний текст ще не оприлюднений, ми можемо послуговуватися проєктом, який розглядав Кабінет Міністрів України.<sup>54</sup> Серед її фокусів – **«перегляд та вдосконалення законодавства з питань відповідальності за поширення дезінформації для збільшення впливу на державу-агресора і мінімізації шкоди для своїх національних інформаційних інтересів»**. Також вона передбачає перегляд та вдосконалення законодавства у сфері обмеження доступу або видалення з українського сегмента інтернету інформації, розміщення якої заборонене законом. Можна припустити, що при введенні відповідальності за поширення дезінформації, ця категорія контенту буде віднесена до «інформації, розміщення якої заборонене законом», тож положення про блокування можуть зачепити і вебсайти, які її поширюватимуть. Тому при подальшій імплементації положень Стратегії, у разі набуття нею чинності, варто враховувати стандарти захисту прав людини, що унеможливило б надмірне обмеження свободи вираження поглядів у мережі.

## Пандемія Covid-19: чи була Україна готовою до інфомедії?

Реанімованим натомість стало одне з положень Кодексу України про адміністративні правопорушення, яке передбачало відповідальність за поширювання неправдивих чуток, що можуть викликати паніку серед населення або порушення громадського порядку.<sup>55</sup> Саме про цю статтю 173-1 КУпАП згадали з початком пандемії Covid-19, що охопила світ у 2020 році й продовжується до сьогодні. Її було введено до КУпАП ще у 1990 році Указом

<sup>53</sup> Українська правда, «РНБО затвердила стратегію біозахисту й інформаційної безпеки України» (15 жовтня 2021):

<https://www.pravda.com.ua/news/2021/10/15/7310592/>

<sup>54</sup> Проєкт Стратегії інформаційної безпеки України:

<http://materialy.kmu.gov.ua/d08bb830/docs/cd2d9166/Dodatok.pdf>

<sup>55</sup> Кодекс України про адміністративні правопорушення:

<https://zakon.rada.gov.ua/laws/show/80731-10>

Президії Верховної Ради УРСР.<sup>56</sup> Санкція за порушення її вимог – накладення штрафу від десяти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян (тобто 170-275 гривень) або виправні роботи на строк до одного місяця з відрахуванням двадцяти процентів заробітку. З точки зору трискладового тесту обмеження прав людини, санкція у вигляді штрафу не є непропорційною; втім, органи при притягненні до відповідальності мають належним чином довести ризик настання негативних наслідків серед населення – паніки або порушень громадського порядку – чи вказати на їхнє настання.

Два випадки застосування цієї статті до поширення інформації в інтернеті сталися до початку пандемії (у 2014<sup>57</sup> та 2018<sup>58</sup> роках). Втім, починаючи з 18 березня 2020 року помітна тенденція активізації роботи судів з розгляду справ за цією статтею КУпАП.<sup>59</sup> З того часу в реєстрі вдалося віднайти 123 постанови у справах про адміністративні правопорушення за цією статтею, що стосуються поширення чуток в інтернеті. Зі 123 постанов лише у 36 випадках осіб притягнуто до відповідальності. Здебільшого ці справи, за рідкісними винятками, стосуються поширення інформації, пов'язаної з коронавірусом. Чимало справ або ж закривали за відсутністю складу адміністративного правопорушення, або ж вони закінчувалися звільненням особи від відповідальності у зв'язку з малозначністю діяння.

Які аргументи переконували суддів у необхідності відмовитися від застосування адміністративної відповідальності? Приклад якісної аргументації можна віднайти в рішенні Жовтневого районного суду міста Дніпро: **«обов'язковим елементом об'єктивної сторони адміністративного правопорушення, передбаченого ст. 173-1 КУпАП є наслідки у виді гіпотетичної можливості викликати паніку серед населення або порушення громадського порядку. Термін “паніка” визначається як психічний стан людей, раптове замішання, розгубленість, несвідомий, нестримний страх, викликаний дійсною чи уявною небезпекою, що охоплює людину чи багатьох людей, неконтрольоване прагнення уникнути небезпечної ситуації»**.<sup>60</sup> Через те, що у протоколі

---

<sup>56</sup> Указ Президії ВР УРСР «Про відповідальність за дії, спрямовані проти громадського порядку і безпеки громадян»:

<https://zakon.rada.gov.ua/laws/show/9082-11>

<sup>57</sup> Постанова Гребінківського районного суду Полтавської області у справі № 528/625/14-п від 8 травня 2014 року:

<https://reyestr.court.gov.ua/Review/64845888>

<sup>58</sup> Постанова Мукачівського міськрайонного суду Закарпатської області у справі № 303/2729/18 від 10 травня 2018 року:

<https://reyestr.court.gov.ua/Review/73879663>

<sup>59</sup> Постанова Лисичанського міського суду Луганської області у справі № 415/1988/20 від 18 березня 2020 року:

<https://reyestr.court.gov.ua/Review/88440335>

<sup>60</sup> Постанова Жовтневого районного суду міста Дніпропетровська у справі № 201/3664/20 від 21 квітня 2020 року:

<https://reyestr.court.gov.ua/Review/90183369>

не зазначено наслідків, до яких могло призвести поширення інформації, суд закрив провадження у справі.

З одного боку, практика справді є непослідовною: у багатьох випадках суди карали за поширення інформації, яка хоч і була недостовірною на момент розповсюдження, ставала достовірною на момент притягнення до відповідальності, зокрема щодо пом'якшення карантину.<sup>61</sup> Часом суди доходили різних висновків щодо притягнення до відповідальності за однаковий контент.<sup>62</sup> Можна зустріти і притягнення до відповідальності користувачів, які розмістили інформацію на своїй сторінці, бо не знали, як показати її колегам на роботі.<sup>63</sup> В одному випадку особа, яку притягнули до відповідальності, стверджувала, що поширила пост як жарт на 1 квітня.<sup>64</sup> У багатьох рішеннях не вказується зміст інформації, за розповсюдження якої особу притягнули до відповідальності.

З іншого боку, ці рішення спростовують тренд кримінального переслідування за поширення висловлювань, що загрожують національній безпеці, – а саме відсутність аналізу висловлювань та наслідків, які вони можуть спричинити.<sup>65</sup> Ба більше, в одному рішенні суддя зважив і на те, що інформація була поширена у «Вконтакте», зазначивши: **«В той же час, вважаю, що таке повідомлення, попри його неправдивість, не могло викликати у людини нестримний страх чи неконтрольоване прагнення уникнути небезпечної ситуації (викликати паніку). Соціальна мережа “Вконтакте” не має широкого поширення серед населення України, оскільки з травня місяця 2017 року в Україні діє заборона на російську соціальну мережу “Вконтакте” шляхом блокування інтернет-провайдером доступу до вказаного сайту».**<sup>66</sup> Це доводить, що судді аналізують

---

<sup>61</sup> Постанова Тернівського районного суду міста Кривого Рогу у справі № 215/2941/20 від 18 травня 2020 року: <https://reyestr.court.gov.ua/Review/89312416>

<sup>62</sup> Серед іншого: Постанова Тернівського районного суду міста Кривого Рогу у справі № 215/2941/20 від 18 травня 2020 року:

<https://reyestr.court.gov.ua/Review/89312416>;

Постанова Красногвардійського районного суду міста Дніпропетровська у справі № 204/2697/20 від 29 травня 2020 року:

<https://reyestr.court.gov.ua/Review/89586737>;

Постанова Красногвардійського районного суду міста Дніпропетровська у справі № 204/3148/20 від 28 липня 2020 року:

<https://reyestr.court.gov.ua/Review/90727909>

<sup>63</sup> Постанова Тернівського районного суду міста Кривого Рогу у справі № 215/2941/20 від 18 травня 2020 року:

<https://reyestr.court.gov.ua/Review/89312416>

<sup>64</sup> Постанова Городищенського районного суду Черкаської області у справі № 691/328/20 від 17 квітня 2020 року:

<https://reyestr.court.gov.ua/Review/89095322>

<sup>65</sup> Віта Володовська, Максим Дворовий, «Інтернет-свобода в Україні 2020: Дотримання прав людини та основоположних свобод в Інтернеті» (Лабораторія цифрової безпеки, 2021):

<https://dslua.org/publications/internet-svoboda-v-ukraini-2020-zvit/>

<sup>66</sup> Постанова Павлоградського міськрайонного суду Дніпропетровської області у справі № 185/3205/20 від 10 червня 2020 року: <https://reyestr.court.gov.ua/Review/89720810>

шкідливий контент та оцінюють вплив на користувачів внаслідок його поширення у мережі.

Фокус цієї норми на шкідливих наслідках для суспільних інтересів внаслідок поширення неправдивої інформації може слугувати прикладом для законодавчого дизайну будь-яких дефініцій, пов'язаних з можливим обмеженням поширення дезінформації як категорії забороненого контенту. Тому ця норма КУпАП має потенціал стати основою для подальшого розроблення дефініції дезінформації відповідно до вимог Стратегії інформаційної безпеки, з уточненням суспільних інтересів, які вона захищатиме. І хоча практика судів у цих справах все ще потребує уніфікації, українським судам також варто запозичити підходи до розгляду справ за статтею 173-1 КУпАП – а саме аналіз контенту та наслідків, до яких його поширення може призвести, – до інших справ щодо розповсюдження протиправного контенту в мережі.

## Українські інституції для протидії дезінформації

Як можна побачити з досвіду іноземних держав та міжнародних організацій, іншим шляхом протидії дезінформації є створення органів влади, які системно працюватимуть у цій сфері. У цій частині дослідження варто повернутися до проєкту Закону про протидію дезінформації.<sup>67</sup> Його положеннями вводилася посада Уповноваженого з питань інформації. Він мав би призначатися на посаду Кабінетом Міністрів України та захищати український інформаційний простір та суспільні інтереси від поширення дезінформації та недостовірної інформації. До його повноважень у цій сфері належали б:

- складання висновків про наявність ознак дезінформації у певному контенті;
- звернення до поширювачів інформації з заявами про відповідь або про спростування дезінформації через електронну систему довіри;
- звернення до суду з позовами про визнання певної інформації дезінформацією, відповідь на неї або ж її спростування;
- звернення до суду про обмеження доступу до інформації, поширеної в інтернеті;
- звернення до суду щодо накладення штрафів, передбачених законопроєктом;
- участь як третьої сторони у всіх справах, пов'язаних зі спростуванням недостовірної інформації.

<sup>67</sup> Порівняльна таблиця законопроєкту:  
[https://mkip.gov.ua/files/pdf/Disinformation\\_Draft\\_2020.pdf](https://mkip.gov.ua/files/pdf/Disinformation_Draft_2020.pdf)



Його повноваження критикувалися з низки підстав. По-перше, заяви про відповідь чи спростування зі сторони Уповноваженого ставали обов'язковими для поширювачів інформації, а механізмів відмови Уповноваженому у праві на відповідь взагалі не передбачалося. По-друге, аналогічний характер носило й маркування матеріалів, які б Уповноважений перевіряв на достовірність та відповідність законодавству. Незрозумілою була і вимога обов'язкового залучення Уповноваженого як третьої сторони у справах про спростування недостовірної інформації, адже його роль у підтримці однієї зі сторін могла б поставити під сумнів рівність сторін у змагальному процесі.<sup>68</sup> Втім, як вже зазначалося, зі зміною складу Кабінету Міністрів України та реорганізацією МКМС у Міністерство культури та інформаційної політики (МКІП) у публічній площині законопроект більше не виринав.

Після невдалої практики створення законопроекту про протидію дезінформації та запровадження посади Уповноваженого з питань інформації, фокус органів державної влади в Україні змістився на формування органів, які мали б працювати у сфері стратегічних комунікацій та протидіяти поширенню шкідливих інформаційних впливів. Цей фокус зберігається і у проєкті Стратегії інформаційної безпеки, який визначає пріоритетом державної політики до 2025 року створення системи протидії дезінформації, інформаційним операціям та атакам, а також системи раннього виявлення, прогнозування та запобігання гібридним загрозам.<sup>69</sup>

Мова про створення у Києві штаб-квартири міжнародного офісу з протидії дезінформації та пропаганди йшла у виступі Президента України Володимира Зеленського на сесії Генеральної асамблеї ООН у вересні 2020 року.<sup>70</sup> Про плани сформувати такий центр при Міністерстві культури та інформаційної політики у лютому 2021 року заявив міністр Олександр Ткаченко<sup>71</sup>, а Володимир Зеленський повторив цю думку в березні.<sup>72</sup>

---

<sup>68</sup> Віта Володовська, Людмила Опришко, Максим Дворовий, Олександр Бурмагін, «Юридичний аналіз законопроекту про дезінформацію» (Лабораторія цифрової безпеки, 23 січня 2020): <https://dslua.org/publications/yurydychnyy-analiz-zakonoproektu-pro-dezinformatsiiu/>

<sup>69</sup> Проєкт Стратегії інформаційної безпеки України: <http://materialy.kmu.gov.ua/d08bb830/docs/cd2d9166/Dodatok.pdf>

<sup>70</sup> Радіо Свобода, «Зеленський в ООН запропонував створити в Києві штаб-квартиру міжнародного офісу з протидії дезінформації» (23 вересня 2020): <https://www.radiosvoboda.org/a/news-zelenskyi-onn/30854567.html>

<sup>71</sup> Укрінформ, «МКІП планує створити Центр протидії дезінформації для боротьби з фейками РФ» (6 лютого 2021): <https://www.ukrinform.ua/rubric-politics/3185864-mkip-planue-stvoriti-centr-protidii-dezinformacii-dla-borotbi-z-fejkami-rf.html>

<sup>72</sup> Інтерфакс-Україна, «Центр протидії дезінформації розпочне роботу в Україні найближчим часом – Зеленський» (9 березня 2021): <https://ua.interfax.com.ua/news/general/728902.html>

Зрештою, 11 березня 2021 року секретар Ради національної безпеки і оборони України оголосив про створення Міжнародного центру протидії дезінформації.<sup>73</sup> 19 березня Президент видав указ про створення цього центру як робочого органу РНБО.<sup>74</sup> МКІП оголосив про призначення на посаду голови Центру стратегічних комунікацій та інформаційної безпеки Любові Цибульської<sup>75</sup>, а 31 березня окреслив основні напрями роботи.<sup>76</sup> 1 квітня генеральний директор «Укрінформу» затвердив Положення про Головну редакцію «Центр стратегічних комунікацій та інформаційної безпеки».<sup>77</sup> 6 квітня керівниця центру при РНБО Поліна Лисенко презентувала основні напрями діяльності цього органу.<sup>78</sup> 7 травня 2021 року указом Президента затверджено Положення про Центр протидії дезінформації.<sup>79</sup> З цього моменту можна вважати закінченим формування нормативної бази для функціонування обох українських центрів протидії дезінформації.

У чому полягає принципова різниця між ними? Певних висновків можна дійти вже з огляду на відмінність у їхніх статусах: центр при РНБО є його робочим органом, в той час, як центр при МКІП працює у формі підрозділу інформаційного агентства. Правовий статус та можливість створення першого передбачені Законом України «Про Раду національної безпеки і оборони України» для **«опрацювання і комплексного вирішення проблем міжгалузевого характеру, забезпечення науково-аналітичного та прогностичного супроводження діяльності»** Ради.<sup>80</sup> Другий центр діє як підрозділ державного інформаційного агентства «Укрінформ» – організації, метою якої є надання інформаційних послуг.<sup>81</sup> Тож повною мірою державним органом можна вважати лише центр

---

<sup>73</sup> Детектор Медіа, «РНБО створила Міжнародний центр протидії дезінформації» (11 березня 2021): <https://detector.media/infospace/article/185723/2021-03-11-rnbo-stvoryla-mizhnarodnyy-tsentr-protydii-dezinformatsii/>

<sup>74</sup> Указ Президента України № 106/2021 Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: <https://www.president.gov.ua/documents/1062021-37421>

<sup>75</sup> МКІП, «Центр стратегічних комунікацій та інформаційної безпеки при МКІП очолить Любов Цибульська» (19 березня 2021): <https://mkip.gov.ua/news/5182.html>

<sup>76</sup> Детектор Медіа, «Напрями та принципи роботи Центру стратегічних комунікацій та інформаційної безпеки (ПРЕЗЕНТАЦІЯ)» (31 березня 2021): <https://detector.media/infospace/article/186524/2021-03-31-napryamy-ta-pryntsypy-roboty-tsentru-strategic-hnykh-komunikatsiy-ta-informatsiynoi-bezpeky-prezentatsiya/>

<sup>77</sup> Отримане у відповідь на запит на доступ до публічної інформації

<sup>78</sup> Детектор Медіа, «Поліна Лисенко презентувала Міжнародний центр протидії дезінформації (ВІДЕО)» (6 квітня 2021): <https://detector.media/infospace/article/186710/2021-04-06-polina-lysenko-prezentovala-mizhnarodnyy-tsentr-protydii-dezinformatsii-video/>

<sup>79</sup> Указ Президента України № 106/2021 «Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: <https://www.president.gov.ua/documents/1062021-37421>

<sup>80</sup> Закон України «Про Раду національної безпеки і оборони України»: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80>

<sup>81</sup> Статут Українського національного інформаційного агентства «Укрінформ»: <https://static.ukrinform.com/files/1606830854-8568.pdf>



при РНБО; центр МКІП за організаційно-правовою формою не може отримувати жодних владних повноважень та виконувати функції органів державної влади.

Якщо заглибитися в установчі документи обох центрів, то можна віднайти ще більше речей, які підтверджують ці відмінності. Так, основним завданням центру МКІП у сфері протидії дезінформації визначено проведення інформаційних кампаній, створення і ведення онлайн-ресурсу, що забезпечить реагування на інформаційні атаки та пояснення ворожих операцій, а також створення та ведення єдиної інформаційної бази присутності агресора.<sup>82</sup> Фактично, ці функції притаманні медіа або ж фактчекінговим організаціям, що вже активно діють та розвінчують фейки.

Центр при РНБО має займатися аналізом і моніторингом подій та явищ в інформаційному просторі України, виявляти загрози для інформаційної безпеки України, а також виконувати прогностичну функцію. Він також повинен аналізувати міжнародний досвід з протидії дезінформації та готувати пропозиції щодо його подальшого впровадження в Україні. Втім, найцікавішими є його повноваження щодо надання пропозицій РНБО в низці сфер, а саме:

- визначення концептуальних підходів у сфері протидії дезінформації та деструктивним інформаційним впливам і кампаніям;
- координації діяльності та взаємодії органів виконавчої влади з питань національної безпеки в інформаційній сфері, забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою;
- здійснення системних заходів, спрямованих на посилення спроможностей суб'єктів сектору безпеки та оборони, інших державних органів задля забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою, розвитку національної інфраструктури у відповідній сфері;
- удосконалення системи правового та наукового забезпечення інформаційної безпеки, виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою.<sup>83</sup>

---

<sup>82</sup> Отримане у відповідь на запит на доступ до публічної інформації.

<sup>83</sup> Указ Президента України № 187/2021 «Питання Центру протидії дезінформації»:  
<https://www.president.gov.ua/documents/1872021-38841>

Вочевидь, цей орган справді працюватиме передусім як аналітичний центр при РНБО, який проводитиме дослідження для подальшого впровадження органом у сфері протидії пропаганді, яка згадана у Стратегії національної безпеки як одна з загроз національній безпеці.<sup>83</sup> Важливим є питання прозорості його діяльності та досліджень, які, за винятком інформації, що містять державну таємницю, мають бути належно оприлюднені для широкого загалу.

Оцінювати діяльність цих органів дещо зарано. Центр стратегічних комунікацій та інформаційної безпеки, що діє при МКІП, активно працює як медіа, спростовуючи дезінформацію та намагаючись на своїй сторінці промотувати український інформаційний продукт та українські наративи. Вони також співпрацюють з представниками громадянського суспільства та українськими медіа задля виконання своїх функцій.<sup>85</sup> У вересні 2021 року<sup>87</sup> Центром було запущено Telegram-канал та сайт під брендом SPRAVDI.<sup>88</sup> На цих ресурсах Центр публікує власні дослідження та аналітику.

Про діяльність Центру протидії дезінформації при РНБО відомо менше: його сторінка у Фейсбукі не оновлювалася з травня по кінець жовтня 2021 року<sup>89</sup>, а єдиною новиною про діяльність довгий час була заява секретаря РНБО про те, що над його запуском працює команда з різноманітних органів державної влади.<sup>90</sup> Лише в середині жовтня 2021 року РНБО презентувало Глосарій назв, термінів та словосполучень, які рекомендовано використовувати у зв'язку з тимчасовою окупацією Російською Федерацією Автономної Республіки Крим, м. Севастополь і окремих районів Донецької та Луганської областей, розроблений за участі Центру.<sup>91</sup> Центр також представив звіт щодо просування проросійських наративів у кількох Telegram-каналах.<sup>92</sup>

---

<sup>84</sup> Указ Президента України № 392/2020 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України”»:  
<https://zakon.rada.gov.ua/laws/show/392/2020>

<sup>85</sup> <https://www.facebook.com/StratcomCentreUA/>

<sup>86</sup> Укрінформ, «Центр стратегічних комунікацій запустив власний сайт»:  
<https://www.ukrinform.ua/rubric-antifake/3319297-centr-strategicnih-komunikacij-zapustiv-vlasnij-sajt.html>

<sup>87</sup> <https://t.me/spravdi>

<sup>88</sup> <https://spravdi.gov.ua/>

<sup>89</sup> <https://www.facebook.com/cpd.official/>

<sup>90</sup> Укрінформ, «Данілов розповів, як запускають Центр протидії дезінформації» (18 червня 2021):  
<https://www.ukrinform.ua/rubric-polytics/3267259-danilov-rozpoviv-ak-zapuskaut-centr-protidii-dezinformacii.html>

<sup>91</sup> Глосарій назв, термінів та словосполучень, які рекомендовано використовувати у зв'язку з тимчасовою окупацією Російською Федерацією Автономної Республіки Крим, м. Севастополь і окремих районів Донецької та Луганської областей:  
<https://www.rnbo.gov.ua/ua/Diialnist/5093.html>

<sup>92</sup> Звіт Центру протидії дезінформації при РНБО України «Антивакцинна пропаганда – інформаційна кампанія проти України»:  
<https://www.rnbo.gov.ua/ua/Diialnist/5111.html>

На цьому етапі важко зрозуміти, чи не виходитиме діяльність Центру при РНБО за рамки, встановлені Конституцією та чинним законодавством. Так, Центр за законом не може безпосередньо впливати на притягнення різноманітних суб'єктів до відповідальності за поширення дезінформації. З іншого боку, РНБО як орган достатньо активно залучена в порушення цифрових прав громадян України через послідовну політику накладення санкцій у вигляді блокувань сайтів. Ця політика у її нинішньому вигляді суперечить вимогам правової визначеності та трискладовому тесту обмежень прав людини, передбаченому міжнародно-правовими документами, а також є непрозорою.<sup>93</sup> Такі блокування не передбачені чинним законодавством України, а обмеження доступу до щонайменше частини заблокованих сайтів не відповідає критеріям пропорційності. Також не опубліковані результати оцінки запровадження санкцій та інформації, що вказувала б на їхню ефективність. Тому існує ризик, що діяльність Центру може бути спрямована як на продовження цієї практики, зокрема шляхом віднайдення більшої кількості ресурсів для блокувань, так і навпаки, для кращої прозорості через зазначення причин обмеження доступу до того чи іншого ресурсу.

## ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

В Україні доволі довго говорять про те, що дезінформація є проблемою, яку необхідно врегулювати законодавчо. Її пеналізація разом з блокуванням ресурсів, де її поширювали, завжди видавалася одним з найлегших та, для деяких політиків, найбажаніших шляхів протидії. Втім, завдяки постійним акцентам зі сторони громадянського суспільства та міжнародних партнерів щодо дотримання прав людини та свободи вираження поглядів, надмірного обмеження цього права в контексті поширення дезінформації у її вузькому сенсі сьогодні в Україні не спостерігається. Інституції ж, створені для протидії дезінформації, досить подібні на свої європейські аналоги і, на перший погляд, спрямовані саме на використання стратегічних комунікацій як інструменту боротьби з умисним поширенням неправдивої інформації з наміром завдати шкоду суспільному інтересу.

Проект Стратегії інформаційної безпеки наголошує на тому, що в майбутньому регулювання поширення дезінформації підлягатиме перегляду. В умовах нинішнього регулювання це означатиме створення відповідної законодавчої системи, яка, згідно з текстом пропонованого проєкту, створюватиме ризики пеналізації поширення дезінформації.

<sup>93</sup> Максим Дворовий, «Санкції та блокування сайтів в Україні: як непомітно відкрити скриньку Пандори» (Лабораторія цифрової безпеки, 2021): <https://dslua.org/publications/sanktsii-ta-blokuvannia-saytiv-v-ukraini-ia-k-nepomitno-vidkryty-skrynku-pandory-analitychnyy-zvit/>

Очевидно, що універсальних механізмів протидії дезінформації не розроблено. Втім, здебільшого вона поширюється в соцмережах. Саме тому будь-яке регулювання, спрямоване на зменшення впливу дезінформації, має концентруватися на соцмережах. Воно має охоплювати:

- зобов'язання на національному рівні компаній, що діють в Україні (зокрема інтернет-посередників), дотримуватися прав людини у своїй діяльності та забезпечити неможливість зловживати цими правами на платформах: у власних правилах користування вони мають закріпити гарантії захисту свободи вираження поглядів, сумісні з міжнародними стандартами у цій сфері, а також створити зручні та зрозумілі для користувача механізми та правила надсилання скарг щодо контенту, який видається їм протиправним;
- передбачення вимог щодо прозорості інформації, яка розміщується на платформах з метою вплинути на суспільну думку, зокрема належне маркування реклами, оприлюднення інформації щодо джерел її походження та її спрямованість на певну цільову аудиторію за прикладом окремих добровільних ініціатив інтернет-платформ щодо політичної реклами та національних прикладів регулювання;
- обмеження або заборону на мікротаргетинг як інструмент, що використовується для зловживань й ампліфікує поширення протиправного контенту, і запровадження прозорості алгоритмів, які використовуються для наповнення особистих стрічок новин у соцмережах;
- розширення можливостей безпосереднього впливу користувачів на порядок та критерії відображення контенту, доступ до якого надає платформа;
- забезпечення гарантій належного процесу (чіткість санкцій, що застосовуватимуться до користувача при поширенні певного контенту, можливість оскаржити рішення про обмеження доступу до контенту чи його депріоритизацію всередині екосистеми платформи тощо) у площині відносин користувач–онлайн-платформа задля можливості перегляду рішень про видалення контенту, що його платформа чи її користувачі маркували як дезінформацію;
- створення або надання повноважень безсторонньому регуляторному органу щодо нагляду за дотриманням платформами нових вимог законодавства.

Україна також має рухатися в напрямку імплементації вимог Digital Services Act, як щодо механізмів захисту прав користувачів та прозорості в широкому сенсі, так і щодо запровадження регулятора і схем співрегулювання, та бути готовою до значних змін регуляторного ландшафту у площині відносин держава–онлайн-платформи після його прийняття на рівні Європейського Союзу. У разі синхронної імплементації DSA з ЄС відкриється можливість заснувати

механізми співрегулювання з такими платформами за участі згаданого вище безстороннього регуляторного органу в цій сфері. Однак ці зміни потребують запровадження комплексного національного регулювання, з огляду на те, що відповідна законодавча інфраструктура на сьогодні відсутня, а її моделювання часто зупиняється на юрисдикційних проблемах.

Роль вже наявних Центрів при РНБО та МКІП має бути подібною до функціоналу Страткомів і подібних органів, що діють при міжнародних організаціях та в деяких країнах. Їхнє завдання – відстежувати та спростовувати наративи, а також продукувати позитивні наративи про Україну. Додатково вони можуть виконувати експертну функцію, приміром, надавати висновки державним органам (регуляторам, судам тощо) щодо наявності умислу та систематичності в поширенні певних наративів. В той самий час ці Центри не повинні перебирати на себе регуляторних та наглядових функцій, які мають належати окремому регуляторному органу, та сприяти продовженню практик сумнівної легальності щодо блокування сайтів.

Разом з тим варто уникнути спроб криміналізувати поширення недостовірної інформації, оскільки цей захід є малоефективним у протидії поширенню дезінформації – як через невідповідність стандартам свободи вираження поглядів, так і через тривалість розгляду відповідних справ у рамках кримінального провадження. Що ж до потенційних змін до Кримінального кодексу України, то до заборонених дій може належати використання ботів, фейкових акаунтів тощо задля умисного впливу на суспільну думку або ж фінансування дезінформаційних кампаній. Втім, притягнення до відповідальності за такі злочини потребуватиме також належного доведення шкідливого впливу, який використання цих акаунтів чи фінансування відповідних кампаній чинитиме на публічну думку.

---

