Література:

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 28.12.2021 № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text.
3. Про створення Центру протидії дезінформації: Рішення РНБО від 11.03.2021 (введене у дію Указом Президента України від 19 березня 2021 року № 106/2021). URL: https://zakon.rada.gov.ua/laws/show/n0015525-21#n2
4. Деякі питання діяльності Міністерства культури та інформаційної політики : Постанова Кабінету Міністрів України від 16.10.2019 № 885. URL: https://zakon.rada.gov.ua/laws/show/885-2019-%D0%BF#Text.
5. Чорна В. Г. Детермінанта обмежень в адміністративному праві. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. Вип. 14. С. 86-94.

DOI https://doi.org/10.36059/978-966-397-277-0-44

ФРОНЕЗИС МОДЕЛІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В КОНТЕКСТІ ГЛОБАЛІЗАЦІЙНИХ ВИКЛИКІВ

Юзікова Наталія Семенівна
доктор юридичних наук, професор,
професор кафедри адміністративного і кримінального права
Дніпровський національний університет імені Олеся Гончара
м. Дніпро, Україна

Глобалізація є об’єктивнім, природним процесом, що пов’язаний з існуванням і розвитком людства, проблеми функціювання екосистеми, світової цивілізації в умовах техногенного прогресу. Глобалізаційні процеси охоплюють різні сфери суспільного життя мають позитивний зміст. Поряд з цим вони супроводжуються ризиками і загрозами. Позитивною складовою глобалізації здебільшого, є явища економічного, політичного характеру (підвищення економічного потенціалу країни, політичне співробітництво, міжнародна співпраця),

негативною – зростання рівня злочинності, підвищена небезпека дезінформації тощо. Однак незважаючи на ці фактори безперечним фактом є зростання та невідворотність процесів глобалізації у світі. Тому питання глобалізації набуває особливої актуальності у контексті формування моделі інформаційної безпеки.

Державна політика у сфері національної безпеки спрямована на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями (п. 4 ст. 3 Закону України Про національну безпеку України).

Інформаційна безпека може розглядатись у дуалістичній площині: як елемент національної безпеки та у якості інтегрованого елементу іншої безпеки: воєнної, економічної, політичної тощо.

Рівень захисту інформаційної безпеки виступає показником розвитку країни, фактором її високого економічного, політичного стану, що спрямовані на забезпечення національних інтересів. Пріоритетом державної політики у сфері інформаційної безпеки виступає захищеність життєво важливих прав і свобод людини і громадянина. Особливої актуальності питання інформаційної безпеки та протидії дезінформації набули в умовах збройного конфлікту.

Фронезис у сфері інформаційної безпеки це послідовність дій орієнтованих на прагматичне звання про добре і погане для людини, розкриття сутності корисного і шкідливого у інформаційному просторі. Сьогодні щохвилини на YouTub завантажується по 72 години відео, у Twitter публікується 100 000 нових твітів, у у Facebook – 700 000 нових коментарів. При такому потоці інформації виникає законне запитання, який відсоток цього контенту є корисним для особи, суспільства, держави, який є добром, а який спричиняє шкоду? Враховуючи, що у цивілізованих країнах кількість інтернет-користувачів – понад 50% населення цих країн, фронезис інформаційної безпеки (практична мудрість), виокремлення корисного і нешкідливого контенту є важливим завданням сьогодення, що сворює умови безпечного розвитку людини, держави і суспільства. Так у Великобританії кількість інтернет-користувачів, становить 92, 6%, Германії 88%, Данії 96,3%, Італії 65,6%, Ісландії 100%, Іспанії 82,2%, Латвії 76,3%, Литві 77,2%, Естонії 91,4%, Нідерландах 93,7%, Польщі 72,4%, Китаї 721434547 (52,2%), США 88,5%, Фінляндії 92,5%, Франції 86,4%, Чеській Республіці 88,4%, Україні 44,1%, Японії 91,1%, Швейцарії 87,2%, Швеції 93,1%. У такому масиві інформації першочергового значення набуває фронезис – здатність приймати вірне рішення на рівні особи, суспільства та держави щодо корисної складової інформації. Фронезис Аристотеля орієнтований на дію, прагматичне знання в основі яких

конкретні випадки, а не загальні правила. Отже практичні навички потрібно розробляти виходячи з конкретних фактів спотворення інформації різних видів інформації, яку можна назвати фейковою. Так, у дослідженні для Ради Європи Клер Уордл та Хосейн Дарахшан виокремлюють три види інформації, яку можна назвати фейковою: 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.

Розвиток новітніх технологій у сфері масової комунікації в Україні та світі детермінує відповідні глобальні ризики і загрози. Одним із найскладніших і небезпечних викликів сьогодення виступає дезінформація. Значна загроза міститься у повідомленнях країни-агресора, а саме: про готовність застосовувати «брудну бомбу», про інсценування події у Бучі, Бородянці, Ізюмі, Херсоні тощо. Відповідну небезпеку становить інформація про безпечність або відсутність проблеми COVID-19, про небезпечність вживання окремих видів наркотичних засобів чи прекурсорів, про наявність залежності від наркотиків чи алкоголю одного з конкурентів на виборах різного рівня.

Головною рисою дезінформації, що відрізняє її від звичайної недостовірної, викривленої інформації, є умисел на її створення. В Енциклопедії Сучасної України під дезінформацією розуміється спотворена, свідомо неправдива, провокаційно-тенденційна інформація, поширена як правдива з метою введення в оману громадськості, політичних опонентів, конкурентів тощо. Також, дезінформацією називається сам процес поширення у ЗМІ чи у інший спосіб викривлених або свідомо неправдивих відомостей. Тобто, дезінформація – це неправдива, оманлива, маніпулятивна інформація, створена навмисне заради економічної, політичної або іншої вигоди. А в умовах збройної агресії РФ дезінформація виступає прямою загрозою життю та здоров'ю людини, безпеці суспільства, суверенітету держави тощо.

Аналізуючи дезінформацію треба виокремити критерії, за якими досліджується її природа, на цьому має базуватись формування моделі фронезису інформаційної безпеки. За приклад можна взяти Рабатський план дій щодо заборони пропаганди національної, расової або релігійної ненависті, що представляє підбурювання до дискримінації ворожнечі або насилля (ООН), який виділяє такі критерії для аналізу висловлювань насильницького характеру (мови ненависті та ворожнечі), що підлягають переслідуванню у кримінально правовому

порядку: контекст, оратор, наміри, зміст та форма, ступінь публічності, ймовірність реалізації заклику до ворожнечі.

Дезінформація поширюється тими ж шляхами, що й будь-яка інша інформація: телебачення, радіо, Інтернет, друковані матеріали (як медіа, так і брошури, буклети тощо). Тому фронезис інформаційної безпеки повинен відповідати тим же критеріям та джерелам інформації. Контекст дезінформації впливає на її дієвість і сприйняття на рівні особи, суспільства та держави. Важливого значення у протидії дезінформації набуває відповідний інформаційний контекст, що охоплює період поширення інформації, таймінг, прогнозовану реакцію кінцевого бенефіціара, середовище тощо. Так, наприклад, фейки, що пов'язані із COVID-19 мають більший вплив на свідомість людини, а відповідно і несуть більшу небезпеку життю та здоров'ю у період пандемій, а дезінформація яка має воєнний контент актуальніша в часі та просторі в умовах воєнного стану, на територіях де відбуваються бойові дії, ворожнеча найкраще розпалюється тоді, коли між сторонами існують певні конфлікти.

Фронезис моделі інформаційної безпеки залежить від форм поширення дезінформації (текстової, відеоконтенту, аудіального контенту) та способів (координована неавтентична поведінка, таргетинг, діпфейки тощо). Найпростіша форма дезінформації – текстова. Адже для написання маніпулятивного тексту (повідомлення) у мережі Інтернет не потрібно фахових навичок монтажу відео, дизайну. Відеоконтент також не представляє складності, тому що для створення примітивного відео достатньо мати смартфон та доступ до інтернету. Якщо колись відео потребувало вираження виключно на телебаченні чи в кінотеатрах, що вимагало часу і витрат на його створення, то зараз відеоблогінг на найпростішому рівні цього не потребує. Сьогодні достатньо мати смартфон та доступ до інтернету. Аудіальний контент, також несе загрози і небезпеку для свідомості суспільства.

Сьогодні найпоширенішим способом дезінформації виступає дипфейк. Так, згідно з дослідженням NewsGuard, вебсайту, що відстежує дезінформацію в інтернеті, найменший контроль за інформацією виявлено у контенті TikTok каналу. Цей спосіб поширення дезінформації працює наступним чином. Користувач знаходить драматичне відео за минулий період (конфлікт, уривок фільму, військові навчання) додає звук потужного вибуху чи інтенсивної перестрілки, запускає пряму трансляцію і, як тільки збереться значна аудиторія, просить фінансову допомогу на підтримку та розвиток свого каналу. Таргетовані повідомлення (які працюють завдяки збиранню інформації про поведінку людини в інтернеті), становлять не меншу небезпеку, а ніж дипфейки, адже можуть використовуватись в умовах

воєнного стану та спричиняти шкоду суспільству та державі. Переважно, «трекінг поведінки» набуває найбільшого розповсюдження під час виборів, але в умовах війни може бути виокремлена соціальна спільнота на яку цілеспрямовано буде подана інформація з дискредитацією ЗСУ, влади, волонтерів, інші повідомлення емоційного характеру з маніпулятивними заголовками тощо. Слід зазначити, що питання захисту персональних даних, актуалізуються у правій площині шляхом отримання згоди (свідомо і явно) користувача щодо використання сайтом файлів «cookies».

Фронезис моделі захисту інформації та протидії дезінформації повинен базуватись на трьох рівнях**:** рівень особи (формування раціонального, критичного мислення на основі принципів свободи вибору; парітетність медіаграмотності та правосвідомості); суспільний рівень (формування якісного інформаційно-аналітичного простору з відповідним контролем за достовірністю інформації; плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, діяльність яких супроводжується належним громадським контролем); державний рівень (активна і реальна протидія свідомій маніпуляції суспільною думкою; формування механізмів виявлення дезінформації і сповіщення про неї, сприяння більшої поінформованості користувачів; впровадження та інформаційно-аналітичне забезпечення політики щодо ідентифікації та неправомірного використання ботів, розповсюдження в мережі оманливої реклами; формування надійної системи захисту персональних даних, задля уникнення «трекінгу поведінки»; запобігання і протидія правопорушенням в інформаційній сфері.

Таким чином, підвищити ефективність реалізації моделей та програм інформаційної безпеки можливо шляхом засвоєння інструментів та методів інформаційного управління та концепції фронезису інформаційного поля виходячи з відповідного рівня (особи, суспільства, держави).