7. Starrett Housing Corporation, Starrett Systems, Inc. and others v. The Government of the Islamic Republic of Iran, Bank Markazi Iran and others. IUSCT Case No. 24. Interlocutory Award (Award No. ITL 32-24-1) – 19 déc. 1983. URL: https://jusmundi.com/fr/document/decision/en-starrett-housing-corporation-starrett-systems-inc-and-others-v-the-government-of-the-islamic-republic-of-iran-bank-markazi-iran-and-others-interlocutory-award-award-no-itl-32-24-1-monday-19th-december-1983 (дата звернення 21.09.2022)
8. Sornarajah M. The International Law on Foreign Investment. 3d. ed. 2010. 556 p.

DOI https://doi.org/10.36059/978-966-397-271-8-67

ГРОМАДЯНСЬКЕ СУСПІЛЬСТВО В УМОВАХ ЦИФРОВІЗАЦІЇ: ВИКЛИКИ ТА ВІДПОВІДІ НА НИХ

Печеранський І. П.
доктор філософських наук, професор,
професор кафедри філософії та педагогіки
Київського національного університету культури і мистецтв
м. Київ, Україна

Загальновідомо, що термін «цифровізація» (англ. «digitalization») вперше використав американський інформатик М. Негропонте у 1995 р. Сьогодні ним оперують у широкому (перехід усіх аспектів економічного та соціокультурного життя на цифрові платформи, драйвер цивілізаційного розвитку) та вузькому (переведення інформації у цифрову форму) значеннях. При цьому, «двигунами» цифрової трансформації постають великі дані (BigData), Інтернет речей (Internet of Things), технології штучного інтелекту та машинного навчання (Artificial Intelligenceand Deep Learning), сучасні біоінженерні технології (Biotech), цифрові двійники (digitaltwins), віртуальна та доповнена реальність (augmented and additivereality), квантовий комп'ютер (Quantum computing), нейромережні технології, «розумні» комплекси та пристрої (smarteverything), системи кібер-безпеки (Cybersecurity), передові матеріали та енергетичні технології та ін.

У 2022 р. впевнено можна констатувати, що цифровізація охопила бізнес, виробництво, науку, соціальну сферу, освіту, побут людей. Вона дісталася навіть до сфер прав людини, громадянського суспільства, взаємин держави і громадян. Останнім часом глобальна мережа перетворилася на середовище реалізації прав, свобод та обов'язків,

державно-владних функцій, що дає підстави вбачати у ній алгоритм соціального розвитку на сучасному етапі.

Поряд з очевидними перевагами цифровізації (створення нових продуктів, послуг і навіть вражень, підвищення операційної ефективності і продуктивності, доступності актуальної та достовірної інформації, надання сучасних технологій для її обробки) важливо за допомогою соціально-філософського аналізу змінити та розширити контекст розгляду, що дозволяє виявити ризики і загрози цифрових інновацій в світлі проблематики прав людини та громадянина.

Дійсно, завдяки амбівалентності відносин й багатовимірності зв'язків у рамках цифрового середовища вдається певною мірою покращити ситуацію з захистом прав особистості та спростити реалізацію окремих прав людини, тоді як висока швидкість і доступність поширення інформації у глобальній мережі на прикладі лавиноподібних «fakenews» суттєво ускладнює реалізацію права на отримання достовірної інформації. Або звернемо увагу на сферу соціального обслуговування, включаючи системи соціальних виплат, де однією з задач цифрової держави є зіставлення даних з різних джерел для виявлення обману та правопорушень з боку заявників, що також пропонує безмежні можливості для стеження та втручання у приватне життя. Не кажучи про те, що використання алгоритмічних систем у сфері соціального захисту, як і в інших випадках автоматичного (напівавтоматичного) прийняття рішень, може призвести до цифрової дискримінації окремих громадян.

Найуспішніші транснаціональні IT-корпорації – Google, Apple, Facebook і Amazon – зберігають великий обсяг персональних даних користувачів, що створює прецедент для порушення базових прав людини, тим більше, що їхні бізнес-моделі та рішення, які приймаються на їх основі, глибоко інтегровані в життя звичайних людей, що дозволяє накопичувати, обробляти та монетизувати персональну інформацію мільярдів [4].

Або ж проблема кібербулінгу, яка вимагає вирішення і правової відповіді, адже йдеться про організований витік в процесі обробки персональних даних або допустимий рівень втручання у приватне життя людини. Так, у низці країн у пандемійному 2020 р. технології «розумних міст» використовувалися для збору даних про громадян, інформування заражених та контролю їх карантину. Чим більше є даних для подальшого аналізу завдяки технологіям, тим застосування останніх ефективніше для боротьби з пандемією. Але багато урядів виступили з критикою активного застосування цих технологій через надмірне втручання у особисте життя громадян.

Серед основних загроз для прав громадян, спричинених цифровізацією, виділяють наступні: кібератаки та комп'ютерне шахрайство, направлені проти людини, держави та бізнесу; кібербулінг, троллінг та інші агресивні діяння у цифровому середовищі проти громадян;

інформаційні війни задля контролю над цифровим простором й масовою свідомістю; боротьба між транснаціональними цифровими платформами та окремими державами, яка відчутно порушує право на недоторканність приватного життя та ін.

Зарубіжні дослідники пропонують різні варіанти вирішення існуючої проблеми. Лунають заклики про важливість розробки способів захисту від маніпуляцій в мережі Інтернет, створення моделі управління Інтернетом усіма зацікавленими державами, забезпечення рівного доступу кожного до інформації та інформаційних технологій, підвищення інформаційної культури користувачів для оцінки власних ризиків онлайн, необхідне створення механізму захисту прав користувачів у мережі Інтернет.

Американські дослідники А. Бом, Е. Джордж, Б. Сіферс і Ш. Лу вважають, що потрібна правова база для усунення потенційних ризиків конфіденційності персональних даних, яка повинна захищати недоторканність приватного життя користувачів, встановлюючи для правоохоронних органів чіткі правила, котрі визначають, коли та з якою метою вони можуть отримати доступ до інформації [1].

На думку Дж. Скотта, необхідно розробити набір базових правил як на федеральному (національному), так і на місцевому рівнях, що дозволять контролювати передові технології, які використовуються урядами. Саме на федеральному рівні потрібно закріпити базовий захист громадян від надмірного державного моніторингу соціальних мереж та інших доступних даних [3].

Реалізація цих пропозицій передбачає величезну роботу законодавців і безлічі інших структур. Багато закордонних дослідників, міркуючи на спробами вирішення означених проблем на національному рівні, вважають, що тут потрібні консолідовані дії всієї міжнародної спільноти. Приміром, П. Бош у статті «Закон про конфіденційність даних: міжнародна перспектива» вважає, що з метою забезпечення захисту даних у ситуації взаємодії різних правових культур та концептуального розуміння конфіденційності, необхідне міжнародне правове регулювання. Культурні відмінності, що впливають на сутнісне розуміння завдань в ході вивчення, диктують необхідність розробки спільного для всіх поняття конфіденційності [2].

Отже, цифрова трансформація, як має нечувані перспективи, так і тягне за собою загрози правам людини, що потребує вироблення нових заходів щодо їхнього захисту. А це вимагає у XXI ст. вивчення випадків порушення прав людини в цифровому суспільстві та окреслення шляхів ефективного реагування на потенціал усіх драйверів Четвертої промислової революції. При цьому, варто усвідомити, що цю проблему не можна вирішити шляхом простого заперечення чи застосування традиційних методик. Фахівці в різних галузях знань повинні мобілізувати весь свій досвід, щоб адекватно реагувати на ризики та загрози для громадянського суспільства, що несе в собі цифровізація.

Література:

1. Bohm A.S., George E.J., Cyphers B., Lu S. Privacy and Liberty in an Alaways-On, Always-Listening World Review. *The Columbia Science and Technology Law.* 2017. Vol. 19. No. 1. P. 1–45.
2. Boshe P. Data Privacy Law: An International Perspective. *Information and Communications Technology Law.* 2015. Vol. 24. No. 1. P. 118–120.
3. Scott J.D. Social Media and Government Surveillance: The Case for be Er Privacy protections for Our Newest Public Space. *Journal of Business & Technology Law*. 2017. Vol. 12, No. 2. P. 151–164.
4. 'The Great Hack' expert warns that Facebook data-grabbing puts 'power overpeople'. RT. URL: https://www.rt.com/news/465602-great-hack-facebook-data-grab/https://rm.coe.int/algorithms-and-human- rights-en-rev/16807956b5

DOI https://doi.org/10.36059/978-966-397-271-8-68

ПОДОЛАННЯ ГРОМАДЯНСЬКИМ СУСПІЛЬСТВОМ ПРОТИПРАВНОЇ ДІЯЛЬНОСТІ В УМОВАХ НАБЛИЖЕННЯ УКРАЇНИ ДО ЄВРОПЕЙСЬКИХ СТАНДАРТІВ БЕЗПЕКИ

Пиріг І. В.
доктор юридичних наук, професор,
професор кафедри криміналістики та домедичної підготовки
Дніпропетровського державного університету внутрішніх справ
м. Дніпро, Україна

Початок XXI ст. у всьому світі зазнав значних змін у політичній та соціально-економічній сферах. Низка факторів, таких як фінансово-економічна криза, пандемія сприяли поширенню злочинних проявів, збільшенню таких його видів як транснаціональна організована злочинність, кіберзлочинність, торгівля людьми, нелегальна міграція, міжнародний тероризм. Трагедією не тільки українського народу, а й всього громадянського суспільства стала війна проти України, розв'язана тоталітарним режимом Російської Федерації, що призвела до сплеску сепаратизму та екстремізму, порушенню існуючих норм міжнародного права.

Криміногенна ситуація в Україні на сьогодні залишається складною. Окрім кримінальних правопорушень загальнокримінальної спрямованості, кількість яких не зменшилась, додались нові види злочинів. За даними Офісу Генерального прокурора за період повномасштабного вторгнення станом на 18.10.2022 року зареєстровано 40601 воєнних та 18020 злочинів проти національної безпеки [1]. Зважаючи на це, протидія