УДК 061.1ЄС
DOI: 10.31733/15-03-2024/2/318-321

Євгенія КОВАЛЕНКО-МАРЧЕНКОВА
начальник
науково-редакційного відділу,
кандидат економічних наук, доцент

Андрій САМОТУГА
заступник начальника
науково-редакційного відділу
Дніпропетровського державного
університету внутрішніх справ,
кандидат юридичних наук, доцент

ЕКОНОМІКО-ПРАВОВІ ЗАХОДИ ЄС У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ОРІЄНТИРИ ДЛЯ УКРАЇНИ

23 червня 2023 р., на другому році повномасштабної російської збройної агресії Україна отримала статус кандидата на членство у ЄС, що стало ще однією важливою віхою на шляху євроінтеграції нашої держави поряд із підписанням нею 27 червня 2014 р. Угоди про асоціацію з ЄС.

Ще до України та Молдови статус кандидата на членство у ЄС у різні роки отримали Албанія (2014), Боснія і Герцеговина (2003), Північна Македонія (2005), Сербія (2012), Туреччина (1999) і Чорногорія (2010). Перемовини про приєднання до ЄС було розпочато з Туреччиною, Сербією, Чорногорією та Албанією. Втім із Туреччиною перемовини призупинено через непідписання нею угоди про асоціацією. Під питанням також перемовини із Сербією через її неприєднання до антиросійських санкцій у зв'язку з війною в Україні. Після найбільшого за територією та населенням розширення ЄС у 2004 р., коли до нього приєдналося 10 країн, процес прийняття нових членів поступово сповільнювався: 2007 р. – Болгарія та Румунія, 2013 р. – Хорватія. Тобто з 2014 р., а саме після початку відкритої гібридної агресії рф проти України процес розширення ЄС призупинився. З яких причин: простого небажання членів ЄС приймати нових чи інші проблеми всередині самого ЄС? Намагатимемося з'ясувати.

Вже у другій половині нульових років, тобто після приєднання Румунії та Болгарії, в архітектурі ЄС з'явилися перші тріщини внаслідок світової фінансової кризи, що позначилося насамперед різким збільшенням внутрішнього боргу та безробіття, особливо серед молоді. Наступними дошкульними ударами для ЄС виявилися міграційні навали 2011-го і подальших років через наслідки «арабської весни», війни в Сирії та виводу американських військ з Афганістану. Згодом міграційна криза поглибилася через російсько-українську війну 2022 р. Не останнім чинником послаблення європейської єдності виявилися такі складові гібридної війни, як інформаційні атаки росії через зловживання нею свободою слова та просування пропаганди й дезінформації, що зумовило прихід до влади і здобуття парламентських місць якщо не відверто антиукраїнськими, то принаймні відчутно проросійськими політичними силами і рухами, що, сповідуючи ксенофобські та расистські гасла, просувають ідеї скорочення або, взагалі, скасування фінансово-економічної та військової підтримки України у її протистоянні з ядерною терористичною державою. Використовуючи існуючі шпарини в європейському та національному законодавстві, росія розпочала інформаційну агресію за допомогою традиційних медіа – радіо й телебачення, але після закриття в багатьох країнах ЄС її іномовних телеканалів «Russia Today» і «Life News» перейшла до ведення інформаційної війни в кіберпросторі, зокрема через соціальні мережі у поєднанні з новітніми ІКТ.

Загалом, технологічний розвиток завжди чреватий несподіванками. Передбачити, на що з часом перетвориться той чи інший стартап, іноді буває неможливо. Наприклад, створюючи Facebook, Марк Цукерберг не уявляв, що його інноваційна ідея, яка, на його думку, повинна об'єднувати людей, стане платформою поширення фейків та маніпуляцій. Через це проблема регулювання цифрового простору постає більш ніж гостро. Сучасне правове поле не завжди вчасно реагує на проблеми, що виникають при впровадженні

певних технологій. У такому випадку технологічним компаніям доводиться застосовувати тактику стримування, тобто відмовлятися від розвитку самої технології. Інший шлях – прийняття законів, що регулювали б її застосування [1].

На загострення проблем інформаційної безпеки в ЄС було звернуто увагу ще під час пандемії коронавірусу 2020-2021 рр. Тоді в одному з аналітичних звітів зазначалося, що відкритість публічної сфери західних суспільств, у поєднанні з економічною глобалізацією, вільним пересуванням через кордони та можливістю прямого доступу до громадян за допомогою транскордонних ІКТ зробила їх вразливими до зовнішнього втручання, що дії ЄС та європейських країн мають переважно захисний характер; не існує ані усталеного підходу до протидії новітнім загрозам, ані чітко визначеної термінології. Ба більше, Європа постала перед значним викликом у технологічній сфері і європейські експерти зазначають, що на сьогодні вона швидше є полем бою, аніж самостійним гравцем. Тільки одна з 20-и найбільших технологічних компаній світу є європейською (Німеччина). На ринку домінують американські та китайські фірми. Наполягання США, що у конкуренції технологій Європа має обирати між США та Китаєм на користь США створює напруженість у стосунках. А ініціатива «Чиста мережа» щодо розвитку мереж 5G, яку в останній рік президентства Д. Трампа оголосив Держсекретар М. Помпео, не мала одностайної підтримки в Європі. Якщо Британія приєдналася до цієї ініціативи США, то Франція та Німеччина продовжували внутрішні дебати і лише обіцяли приєднатися. Деякі країни західних Балкан не зробили жодного кроку в цьому напрямку. Між Європою та США також існує непорозуміння у сфері оподаткування тих гігантів, що отримують прибутки на місцевих ринках, а податки платять у США. У багатьох країнах вони присутні лише у віртуальному просторі, але займають велику частку рекламного ринку, чим підривають доходи традиційних медіа [2].

Повномасштабна війна росії проти Україні змусила європейських політиків та економістів до радикалізації заходів щодо інформаційної безпеки насамперед у межах ЄС, адже інформаційні загрози передовсім мають економічні, соціальні, культурно-психологічні та військові наслідки. Першими з таких кроків стало прийняття Європарламентом і Радою двох важливих актів: 14 вересня 2002 р. – Закону про цифрові ринки (DMA – Digital Markets Act), імплементація якого розпочалася 17 лютого 2023 р., та 19 жовтня 2022 р. – Закону про цифрові послуги (DSA – Digital Services Act) з імплементацією на початок березня 2023 р.

DMA спрямований на створення у цифровому секторі більш справедливих та конкурентоспроможних ринків. Для цього цей закон встановлює набір чітко визначених об'єктивних критеріїв для ідентифікації «гейткіперів» – великих цифрових платформ, що надають так звані основні платформні послуги, такі як онлайн-пошукові системи, магазини програм, служби обміну повідомленнями [3]. Гейткіперам доведеться дотримуватися перелічених у DMA вимог і заборон. DMA є одним із перших регуляторних інструментів для комплексного регулювання повноважень найбільших цифрових компаній. DMA доповнює, але не змінює правила конкуренції ЄС, що продовжують застосовуватися в повному обсязі [4].

6 вересня 2023 р. Європейська комісія визначила шість гейткіперів: Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft. Вони мають шість місяців щоб забезпечити повну відповідність зобов'язанням DMA для кожної з призначених ними основних служб платформи. Загалом було визначено 22 основні сервіси платформи, що надають гейткіпери. Відповідно до DMA, Європейська комісія може визначити цифрові платформи як «гейткіперів», якщо вони забезпечують важливий шлюз між підприємствами та споживачами щодо основних послуг платформи. Комісія контролюватиме ефективне виконання та дотримання цих зобов'язань. Якщо гейткіпер не дотримується зобов'язань, встановлених DMA, Комісія може накласти штраф у розмірі до 10 % від загального світового обороту компанії, який може досягати 20 % у разі повторного порушення. У разі систематичних порушень Комісія також має право вживати додаткових заходів правового захисту, такі як зобов'язання гейткіпера продати бізнес або його частини або заборона гейткіперу на придбання додаткових послуг, пов'язаних із системною невідповідністю [5].

Крім того, багато з кількамільйонних штрафів, накладених на ці компанії в результаті адміністративних проваджень, ініційованих ЄС протягом останніх років, були оскаржені в Європейському суді, що підкреслює необхідність удосконалення нормативної бази для цифрових ринків та послуг. Нове регулювання стосуватиметься великих технологічних компаній, що називаються гейткіперами і які більш схильні до недобросовісної конкуренції. До них належать такі послуги, як механізми дослідження, операційні системи, хмарні обчислення, онлайн-реклама, соціальні мережі та платформи

для обміну відео [6].

DSA є найважливішим і найамбітнішим у світі нормативним актом у сфері захисту цифрового простору від поширення незаконного контенту та захисту основних прав користувачів. У світі немає іншого законодавчого акта щодо регулювання соціальних мереж, онлайн-ринків, дуже великих онлайн-платформ (VLOP – very large online platform) і дуже великих онлайн-пошукових систем (VLOSE – Very Large Online Platforms and Search Engines). Правила розроблені асиметрично: більші посередницькі послуги зі значним суспільним впливом (VLOP і VLOSE) підпадають під більш суворі правила.

Після прийняття DSA платформи не тільки мають бути більш прозорими, але й відповідатимуть за свою роль у поширенні незаконного та шкідливого контенту. Серед іншого DSA: 1) встановлює спеціальні зобов'язання для онлайн-ринків з метою боротьби з онлайн-продажем незаконних продуктів і послуг; 2) запроваджує заходи для протидії незаконному контенту в Інтернеті та зобов'язання платформ швидко реагувати, дотримуючись основних прав; 3) захищає неповнолітніх в Інтернеті, забороняючи платформам використовувати цільову рекламу на основі використання персональних даних неповнолітніх, як це визначено законодавством ЄС; 4) накладає певні обмеження на подання реклами та на використання конфіденційних персональних даних для цільової реклами, включаючи стать, расу та релігію; 5) забороняє оманливі інтерфейси, відомі як «темні шаблони», і практики, спрямовані на введення в оману.

Більш суворі правила застосовуються до VLOP і VLOSE, які повинні будуть: 1) запропонувати користувачам систему рекомендацій контенту, яка не базується на профілюванні; 2) проаналізувати системні ризики, що вони створюють: ризики, пов'язані з поширенням незаконного контенту, негативним впливом на основні права, на виборчі процеси та гендерне насильство чи психічне здоров'я.

У контексті російського військового вторгнення в Україну, що супроводжується серйозними та масовими порушеннями прав людини та українського народу, а також особливого впливу на маніпулювання онлайн-інформацією, DSA запроваджує механізм реагування на кризу. Цей механізм дозволить проаналізувати вплив діяльності VLOP і VLOSE на кризу та швидко прийняти рішення про пропорційні та ефективні заходи для забезпечення дотримання основних прав [7].

25 квітня 2023 р. на виконання DSA Європейська комісія прийняла перші рішення, визначивши 17 VLOP і 2 VLOSE, якими щомісяця охоплено принаймні 45 млн активних користувачів. До VLOP віднесено: Alibaba AliExpress, Amazon Store, Apple AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, Zalando. До VLOSE віднесено Bing та Google Search. Після такого визначення компанії тепер протягом чотирьох місяців доведеться виконати повний набір нових зобов'язань згідно з DSA. Вони спрямовані на розширення можливостей і захист користувачів онлайн, включно з неповнолітніми, вимагаючи від призначених служб оцінювати та зменшувати їхні системні ризики та надавати надійні інструменти модерації контенту [8]. Приміром, 19 лютого 2024 р. Єврокомісія відкрила офіційне провадження щоб оцінити, чи міг TikTok порушити DSA у сферах, пов'язаних із захистом неповнолітніх, прозорістю реклами тощо. Водночас DSA не встановлює жодного юридичного терміну для завершення провадження, оскільки тривалість поглибленого розслідування залежить від багатьох факторів, зокрема складності справи, ступеня співпраці відповідної компанії з Комісією тощо.

Отже, однією з причин призупинення розширення ЄС вважаємо намагання євроінституцій навести лад у себе вдома, щоб потім приймати до себе нових членів. А одним із таких заходів є убезпечення інформаційного простору від шкідливих ворожих впливів, що водночас вимагається і від держав-кандидатів. Наприклад, це передбачено Угодою про асоціацію між Україною та ЄС у частині боротьби з кіберзлочинністю та розвитку інформаційного суспільства.

Відповідно до Звіту про виконання Угоди між Україною та ЄС за 2023 рік стосовно захисту персональних даних на розгляді у Верховній Раді України перебувають проєкти законів України «Про захист персональних даних» та «Про Національну комісію з питань захисту персональних даних та доступу до публічної інформації». 01.01.2023 набрав чинності Закон України від 01.12.2022 «Про авторське право і суміжні права», 15.04.2023 – Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності». 10.06.2023 прийнято Закон України «Про захист прав споживачів», що має на меті імплементувати, зокрема, деякі положення Директиви

Європейського Парламенту та Ради № 2000/31/ЄС від 08.06.2000 «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку» («Директива про електронну комерцію»). Україною здійснено також низку інших заходів у сфері цифровізації економіки, розвитку електронного врядування та розширення електронних послуг, удосконалення антимонопольного законодавства та захисту економічної конкуренції, зокрема у кіберсфері [9].

Виконання цих та інших вимог є не лише визначальною умовою для набуття Україною членства у ЄС, а й запорукою подальшого надання їй в умовах війни з боку ЄС та окремих його держав-членів матеріально-фінансової і військової допомоги та здійснення антиросійської санкційної політики. Від часу вторгнення росії ЄС надав Україні економічну, гуманітарну та військову підтримку на суму понад 88 млрд євро [10]. Крім того, на сьогодні ЄС залишається для України єдиним джерелом фінансової допомоги. На початку 2024 р. усі 27 лідерів країн-членів домовилися про додатковий пакет підтримки України в розмірі 50 млрд євро в рамках бюджету ЄС. Адже на тлі блокування виділення грошей від США через політичні суперечки між демократами та республіканцями в Конгресі щодо мігрантів та кордону подальша затримка з виділенням грошей від ЄС могла призвести до серйозних проблем в Україні – не лише військових, а й відсутності зарплат, пенсій та інших критичних витрат.

1. Баловсяк Н. Проти фейків та монополізму. Як змінять Інтернет нові європейські закони (16.08.2022). URL : https://tyzhden.ua/proty-fejkiv-ta-monopolizmu-iak-zminiat-internet-novi-ievropejski-zakony/.

2. Впливи у цифровому просторі: як Європа шукає свій шлях протидії та що може запозичити Україна? Аналітичний звіт. URL : https://ufss.com.ua/wp-content/uploads/2021/06/UFSS_countering_influence.pdf.

3. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925.

4. About the Digital Markets Act. URL : https://digital-markets-act.ec.europa.eu/about-dma_en.

5. The Digital Markets Act (DMA). URL : https://eu-digital-markets-act.com/.

6. DMA & DSA: regulating digital markets and services (06 Feb, 2024). URL : https://www.11onze.cat/en/magazine/dma-dsa-regulating-digital-markets-services/.

7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

8. The Digital Services Act (DSA). URL : https://www.eu-digital-services-act.com/.

9. Звіт про виконання Угоди про асоціацію між Україною та Європейським Союзом за 2023 рік. URL : kmu.gov.ua/zvit-pro-vykonannia-ua-za-2023_UA_2.

10. Підтримка ЄС Україні. URL : https://european-union.europa.eu/priorities-and-actions/eu-support-ukraine_uk.