УДК 342.951

КАЛАЙДА Ю.П., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0002-1408-2145.

ЗАБЕЗПЕЧЕННЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ В УМОВАХ ГЕОПОЛІТИЧНОГО ПРОТИБОРСТВА: КРАЩІ ПРАКТИКИ ЗАРУБІЖНОГО ДОСВІДУ

Анотація. *Розглянуто зміст та особливості цифрового суверенітету. Визначено сучасні тенденції забезпечення цифрового суверенітету в умовах геополітичного протиборства. Висвітлено кращі практики зарубіжного досвіду у сфері забезпечення цифрового суверенітету. Окреслено загрози діяльності соціальних мереж та онлайн-платформ в контексті необхідності розробок вірогідних моделей захисту національного сегменту кіберпростору. Узагальнено питання щодо блокування та видалення деструктивного контенту соціальними мережами. Акцентована увага на питаннях посилення відповідальності глобальних ІТ-корпорацій. Деталізовано шляхи удосконалення вітчизняного законодавства щодо посилення цифрового суверенітету, захисту цифрових прав та свобод громадян. Визначено напрямки унормування діяльності та оподаткування соціальних мереж в Україні.*

Ключові слова: *цифрові технології, національний суверенітет, цифровий суверенітет, кібербезпека, кіберпростір, репост, деструктивний контент, загроза, медіарегулятор, аккаунт, ІТ-корпорація, онлайн-платформа, технологічні трансформації, геополітичне протиборство.*

Summary. *The content and features of digital sovereignty are considered. The modern trends of ensuring digital sovereignty in the conditions of geopolitical confrontation are determined. The best practices of foreign experience in the field of digital sovereignty are highlighted. The threats to the activities of social networks and online platforms in the context of the need to develop plausible models for the protection of the national segment of cyberspace are outlined. The issue of blocking and removing destructive content by social networks is covered. Emphasis is placed on strengthening the responsibility of global IT-corporations. The directions of improvement of domestic legislation on strengthening digital sovereignty, protection of digital rights and freedoms of citizens are detailed. The directions of standardization of activity and taxation of social networks in Ukraine are determined.*

Keywords: *digital technologies, national sovereignty, digital sovereignty, cyber security, cyberspace, repost, destructive content, threat, media regulator, account, IT-corporation, online platform, technological transformations, geopolitical confrontation.*

Аннотация. *Рассмотрены содержание и особенности цифрового суверенитета. Определены современные тенденции обеспечения цифрового суверенитета в условиях геополитического противоборства. Освещены лучшие практики зарубежного опыта в сфере обеспечения цифрового суверенитета. Очерчены угрозы деятельности социальных сетей и онлайн площадок в контексте необходимости разработок возможных моделей защиты национального сегмента киберпространства. Обобщены вопросы блокирования и удаления деструктивного контента социальными сетями. Акцентировано внимание на вопросах усиления ответственности глобальных ИТ-корпораций. Детализированы направления усовершенствования отечественного законодательства в части усиления цифрового суверенитета, защиты цифровых прав и свобод граждан. Определены направления нормирования деятельности и налогообложения социальных сетей в Украине.*

Ключевые слова: *цифровые технологии, национальный суверенитет, цифровой суверенитет, кибербезопасность, киберпространство, репост, деструктивный контент, угроза, медиарегулятор, аккаунт, ИТ-корпорация, онлайн-площадка, технологические трансформации, геополитическое противостояние.*

Постановка проблеми. В умовах інтенсивного та динамічного розвитку цифрових технологій, які характеризуються екстериторіальним характером, останнім часом актуалізуються ризики, загрози та виклики, пов'язані із глобалізацією ключових сфер життєдіяльності сучасних держав та світової спільноти. Не виключається, що екстериторіальний потенціал сучасних цифрових технологій може бути реалізовано зовнішніми гравцями у різноманітних сферах, включаючи такі галузі, як політика та економіка, у зв'язку з чим традиційне уявлення про національний суверенітет перестає адекватно відповідати сучасним умовам технологічного розвитку людства, що, у свою чергу, формує нагальну потребу перегляду класичних підходів до визначення змісту, структури та функцій такого феномену як державний суверенітет.

Суверенітет держави – політико-юридична властивість державної влади, яка означає її верховенство і повноту всередині країни, незалежність і рівноправність у зовнішньополітичній сфері. Правовою основою державного суверенітету є конституції країн, декларації, загальновизнані принципи міжнародного права, які фіксують суверенну рівність держав, їхню територіальну цілісність, невтручання у внутрішні та зовнішні справи, право націй на самовизначення. 16 липня 1990 року Верховна Рада тоді ще Української РСР схвалила фундаментальний акт – Декларацію про державний суверенітет України [1]. Цей акт, який має понад 30-річну історію свого існування, на жаль, питання цифрового суверенітету жодним чином не регламентує. Більш того, за таких умов виникає необхідність визначення й дослідження такого феномену як цифровий суверенітет та його складових.

Аналіз сучасних тенденцій розвитку політичного та соціально-економічного життя надає підстави констатувати, що існує низка нагальних проблем, пов'язаних із встановленням та визнанням цифрового суверенітету у конгломераті формування потреб держав та суспільства. У сфері глобального геополітичного протиборства між технологічно розвиненими державами світу спостерігаються перманентні процеси інформаційного втручання в національні сегменти Інтернет-простору, що надає можливість у віддаленому режимі впливати на функціонування національних політичних режимів, створюючи завдяки інформаційно-комунікаційному впливу на свідомість населення країн-мішеней вигідні моделі масової політичної реальності, що особливо важливо у сучасних умовах. Крім того, завдяки застосуванню цифрових комунікаційних технологій держава-агресор (РФ) та її сателіти можуть здійснювати цілеспрямований підрив соціально-політичної стабільності будь-яких держав світу, які виступають у якості геополітичних опонентів. Тобто на національному рівні РФ залишається супротивником, яка здійснює відкриту збройну агресію проти України, системно застосовуючи політичні, воєнні, економічні, інформаційно-психологічні та кібернетичний потенціал, які загрожують незалежності, державному суверенітету і територіальній цілісності України.

На цьому фоні провідні технологічні платформи ("Google", "Facebook", "Twitter", "YouTube", "Instagram") фактично здійснюють монополізацію цифрового простору, пропонуючи мільярдам користувачів, незалежно від географічного розташування країн у світовому масштабі, достатньо обмежений набір моделей соціально-політичної реальності, здійснюючи при цьому блокування альтернатив, наприклад аккаунти політиків, засобів масової інформації, каналів на відеохостінгу "YouTube" тощо на своїх

сервісах. Таким чином, сучасні процеси зовнішнього інформаційно-комунікаційного втручання у суверенні національні інформаційні простори розглядаються як один із напрямків підриву цифрового суверенітету відносно потенційних держав-мішеней.

В економічній сфері також спостерігаються активні спроби та прагнення вжиття заходів з метою цифрової десуверенізації. Так, цифрова валюта "Bitcoin" та подібні до неї альтернативні криптовалюти створені з метою заміни національних фіантних валют, надають сприятливу можливість їх власникам здійснювати неконтрольовану з боку державних органів будь-яку фінансово-економічну діяльність.

У сфері національної безпеки також відбуваються активні трансформації, які призводять до появи нових сучасних інструментів та сервісів, за допомогою яких інформація зберігається у зашифрованому вигляді на пристроях Інтернет-користувачів та формуються відповідні бази даних, які перебувають у розпорядженні власників соціальних мереж. Це дозволяє обійти контроль та регулятивні правила профільних та спеціальних служб, відповідальних за забезпечення безпеки національних сегментів цифрового простору тієї чи іншої держави. За таких умов, держава втрачає свої монопольні права та традиційні можливості у сфері забезпечення та підтримання національного суверенітету.

Зазначені обставини актуалізують важливість та необхідність висвітлення феномену цифрового суверенітету та загрозливих тенденцій його забезпечення в умовах сучасних глобальних технологічних трансформацій та геополітичного протиборства.

Результати аналізу наукових публікацій. Дослідження правової природи інформаційного суверенітету та його складових здійснювали у своїх наукових працях такі фахівці, як М. Дмитренко [2], О. Довгань [3], І. Доронін [4], О. Ніщименко [5], О. Солодка [6] та інші. Аналіз праць цитованих авторів надає змогу узагальнити загальне розуміння змісту поняття "інформаційний суверенітет" що являє собою невід'ємне право людини, суспільства, держави на самовизначення та участь у формуванні, розвитку і здійсненні національної інформаційної політики. Науковцями констатовано, що це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі. Проте жоден із вказаних науковців не здійснював висвітлення кращих практик зарубіжного досвіду, присвячених проблемам забезпечення цифрового суверенітету, що посилює актуальність обраного тематичного напряму дослідження. Оскільки цифровий суверенітет є різновидом інформаційного суверенітету, то завданням автора є розкриття особливостей його забезпечення у національних сегментах кіберпростору шляхом проведення порівняльно-правового аналізу деяких актів зарубіжного законодавства, необхідність окреслити сучасні загрози у цьому контексті.

Метою статті є висвітлення та узагальнення спроможностей деяких держав світу у сфері забезпечення цифрового суверенітету в умовах глобального геополітичного протиборства.

Виклад основного матеріалу. XXI століття беззаперечно вважається епохою розвитку цифрових технологій. Кардинальну трансформацію проходять традиційні галузі діяльності держави, суспільства, бізнесу. Створюються принципово нові можливості та спроможності для розвитку економіки, соціальної сфери, сектору безпеки і оборони, державного управління тощо. Разом з тим нові технологічні рішення, окрім благополуччя держав та їх населення, породжують нові ризики та загрози. Невипадково в сучасну епоху тотальної діджіталізації актуальним завданням політичного керівництва

багатьох держав світу залишається розробка та схвалення законодавчих ініціатив з метою захисту цифрового суверенітету.

У першу чергу, проголошення та забезпечення цифрового суверенітету або суверенізація Інтернету є правом будь-якої держави світу. Одним з перших визначив поняття цифрового суверенітету французький бізнесмен П'єр Беланжер у 2012 році. На його переконання, "цифровий суверенітет" (*souveraineté numérique*) являє собою "контроль над сьогоднішнім днем", який формується шляхом застосування технологій та комп'ютерних мереж. Одночасно П. Беланжер тлумачить це поняття та його зміст в контексті захисту приватного життя громадян європейських держав у кіберпросторі, зокрема, робить акцент на доцільності прискорення створення власних європейських систем у технологіях Хмарних обчислень та зберігання даних громадян. З цієї позиції Беланжер підтримує запровадження державного контролю даних та систем зв'язку, підкреслюючи необхідність зниження контролю з боку іноземних ІТ-корпорацій.

На цьому фоні уряди багатьох держав світу намагалися підвищити захищеність інтересів держави та громадян шляхом підтримки розвитку національних технологій схваленням відповідних законів. Так, Президент Бразилії Д. Русеф (2011 – 2016 рр.) запропонувала план виходу бразильського сегменту мережі Інтернет з під індустріального впливу США та американських ІТ-корпорацій, що можна вважати реалізацією спроби забезпечення власного цифрового суверенітету. Німеччина з 2015 року ініціювала процес створення власної системи обміну електронними повідомленнями, прокладання нових підводних кабелів та розпочала просування політики локалізації даних з метою протидії американському та російському впливу, особливо після скандалу із зламом особистої електронної пошти канцлера А. Меркель. Після зламу даних французького уряду під час виборчої кампанії у 2017 році Франція спрямувала значні фінанси на розробку власного зашифрованого урядового месенджера з відкритим кодом, що також є спробою встановлення певним чином цифрового суверенітету.

Таким чином, майже усі високорозвинені країни світу визначають доцільність коригування засад національного законодавства з метою гарантування цифрових прав та свобод громадян, забезпечення національного цифрового суверенітету. Хоча існують й радикальні приклади діяльності держави у цьому напрямку. Так держава-агресор (РФ) з 2011 по 2018 роки запровадила практику адміністративного та кримінального переслідування користувачів Інтернету та соціальних мереж за "деструктивні" та "екстремістські" лайки, пости та коментарі. Одночасно з 1 січня 2017 року в РФ був введений податок, який зобов'язав нерезидентів сплачувати податок на додану вартість з продажу на її території електронних послуг: цифрового контенту, послуг зберігання та обробки інформації, реєстрації доменів і хостингу тощо, при цьому вони повинні стати на податковий облік. Серед технологічних гігантів у контролюючому органі зареєструвалися "Apple Distribution International", "Google Commerce","Microsoft Ireland", "Netflix International B.V.", "Wargaming Group", "Bloomberg", "Alibaba", "Booking.com" та ін. Загалом з моменту впровадження податку на податковий облік стало 1580 компаній. Аналогічні податкові правила були введені і в Республіці Білорусь у 2018 році.

Адже у світі щодо цифрового суверенітету склалася біполярна ситуація.

З одного боку, держави прагнуть забезпечити цифровий суверенітет, захистити цифрові права та свободи громадян, гарантувати захист даних, а з іншого – намагаються контролювати дії своїх громадян у кіберпросторі та у соціальних мережах, особливо у питаннях поширення фейків та деструктивного контенту. Щодо останнього, то слід зауважити, що у державах схвалюються законодавчі акти з метою блокування та нівелювання небезпечних проявів у мережі Інтернет або у соціальних мережах. З цього

приводу у Німеччині в 2017 році було прийнято спеціальний законодавчий акт під назвою “The Network Enforcement Act” (NetzDG), який зобов’язує соціальні мережі та інші Інтернет-платформи співпрацювати з державними структурами з метою контролю поширюваного користувачами контенту та запобігання розповсюдженню протиправного або забороненого контенту. Вказаний закон охоплює перелік понад двох десятків різноманітних правопорушень у сфері соціальних мереж, розпочинаючи від закликів до насильницьких висловлювань до поширення фейкових матеріалів. З моменту набуття чинності цим законом інформаційно-комп’ютерні платформи у тому числі й інтернаціональні (“Facebook”, “YouTube”, “Twitter” тощо), зобов’язані блокувати протиправний контент.

У 2020 році Уряд Великобританії поставив перед собою одіозне завдання – створити найбезпечніший у світі онлайн-простір для спілкування користувачів. Очікується, що захист користувачів мають забезпечити саме онлайн-платформи та соціальні мережі. У випадку, якщо користувачі стануть жертвами протиправного контенту, то відповідальність будуть нести саме соціальні мережі, включаючи особисту відповідальність співробітників ресурсу. Запропоновано спеціальний механізм під назвою “Safety by Design”, який надасть змогу впроваджувати в нові продукти під час їх розробки з метою забезпечення безпеки онлайн. Під дію нових ініціатив підпадають усі платформи, які пропонують обмін даними серед користувачів. Перелік загроз, зафіксований у спеціальному документі під назвою “Online Harms White Paper”, поділяється на три категорії: 1) деструктивна інформація, яка має юридичне визначення (пропаганда агресії, заохочення самогубств тощо); 2) шкідлива інформація, яка не має юридичного статусу (тролінг, залякування); 3) легальний контент, не призначений для дітей (ненормативна лексика, додатки сайтів знайомств тощо). У лютому 2020 року Уряд Великобританії вирішив надати національному медіарегулятору “Ofcom” право боротися з шкідливим та протиправним контентом, у тому числі на форумах, відеохостингах та в соціальних мережах. Тобто ця державна структура отримала повноваження з метою кардинальної боротьби за чистоту Інтернету. За таких умов приклад Сполученого Королівства є показовим. Саме соціальні мережі зобов’язані максимально відповідально ставитися до контенту та творчості користувачів. При цьому, як переконливо засвідчує іноземний та міжнародний досвід, ІТ-гіганти, з одного боку, блокують пости та аккаунти за власним баченням (оскаржити таке рішення практично неможливо), а з іншого боку – досить часто ігнорують вимоги користувачів або представників влади тієї чи іншої держави.

Останнім часом у світі спостерігається загрозлива тенденція, за якої свою волю урядам держав нав’язують та диктують гігантські ІТ-корпорації, переважно американські, абсолютно ігноруючи закони та нормативно-правові акти цих країн. У зв’язку з чим у багатьох країнах світу – Італії, Австралії, Індії тощо активно розроблюються пропозиції та впроваджуються заходи з метою боротьби із свавіллям глобальних приватних ІТ-компаній, постачальників соціальних мереж, включаючи заходи з посилення відповідальності. Проблема функціонування соціальних мереж у глобальному вимірі тісно пов’язана із національною безпекою та державним суверенітетом, оскільки саме соціальні мережі останнім часом стали інструментом для проведення так званих “кольорових революцій”. Свого часу після подій, які увійшли в історію людства як “Арабська весна” або “твітер-революція”, кожна країна опікується питаннями планомірного захисту власного сегменту кіберпростору, особливо щодо діяльності соціальних медіа. Саме соціальні мережі виступають одночасно сучасною організаційною зброєю та привабливим бізнес-продуктом. Гігантом серед соціальних

мереж виступає американська транснаціональна корпорація “Facebook”, у якій зареєстровано понад 1,4 млрд. користувачів. Як переконливо демонструє досвід останніх років, американські соціальні мережі роками ігнорують закони інших країн світу. Тому на сьогодні в багатьох країнах світу розроблюються законодавчі ініціативи з метою забезпечення цифрового суверенітету та протидії свавіллю глобальних ІТ-компаній, включаючи запровадження серйозних санкцій.

Досить радикально підійшли до питання правової регламентації діяльності соціальних мереж у Туреччині. В цій країні вперше в історії людства було схвалено Закон “Про соціальні мережі” № 7253 [7], який набув чинності з 1 жовтня 2020 року. На виконання цього законодавчого акта великі Інтернет-платформи, представлені у цій країні, на кшалт “Facebook”, “Twitter“, “Periscope”, “YouTube” и “TikTok”, “Instagram” та інші, які мають аудиторію користувачів понад 1 млн. осіб, зобов’язані відкривати офіційні представництва своїх компаній та призначати уповноважених осіб для взаємодії з органами державної влади та судовими інстанціями Туреччини. Нормативно встановлено, що головою представництва має бути громадянин саме Туреччини. Також законом запроваджена обов’язкова вимога щодо видалення “образливого” контенту протягом 48 годин та зберігання даних турецьких користувачів в соціальних мережах виключно на території Турецької республіки. Таким чином, ресурси зобов’язані видаляти заборонений контент, як тільки його помітить місцевий регулятор – управління телекомунікацій та зв’язку. У листопаді 2020 року великі соціальні компанії “Facebook”, “Twitter”, “Periscope”, “YouTube” и “TikTok” були оштрафовані за невиконання вимог вказаного законодавчого акта на загальну суму 10 млн. турецьких лір. Таким чином, в Туреччині у цьому році з’являться офіційні представництва (локальні офіси) соціальних мереж “Facebook” та “Instagram”. Якщо вимоги закону будуть проігноровані, то соціальна мережа знов може бути оштрафована та запроваджено зменшення або гальмування її трафіку. Локальні офіси соціальних мереж в Туреччині наділені правом призупиняти роботу соціальних мереж та медіа. У Туреччині відкриття представництв “Facebook” та “Instagram” вважають значною перемогою, оскільки такий крок дозволить владі вимагати дотримання місцевого законодавства соціальними мережами. Тоді як відсутність таких представництв сприяє ігноруванню ІТ-компаніями правил ринку та дозволяє ухилятися від податків й штрафів за порушення законодавчих вимог. Іншими словами, турецький прецедент надасть змогу вирішити питання побудови унормованих відносин з американськими цифровим компаніями й в інших країнах світу.

Цікавим у цій площині є досвід Індії – держави, де знаходиться найбільший ринок месенджера “WhatsApp”. Так у 2020 році було розпочато антимонопольне розслідування у зв’язку з обов’язковим оновленням політики конфіденційності “WhatsApp”. На переконання Комісії з конкуренції Індії (Competition Commission of India, CCI) “WhatsApp” порушив місцеві закони про конкуренцію своїми вимогами. Однією із запроваджених новацій стала обов’язковість передачі даних усіх користувачів “WhatsApp” до мережі “Facebook”, що значно обурило багатьох користувачів та як наслідок призвело до збільшення навантаження на конкурентів, зокрема месенджера “Telegram”.

Австралія має намір прийняти закон, який зобов’яже Інтернет-гігантів (таких як “Google” та “Facebook”) сплачувати австралійським виданням гонорари за розміщення новинного контенту на своїх платформах. Новий законопроект про медіаринок став фактичною відповіддю на становище, яке австралійські ЗМІ вважають “несправедливим”. Вони піддають критиці Інтернет-гігантів за те, що ті отримують прибуток з демонстрації новинного контенту і при цьому ніяк не стимулюють фінансово самі видання.

ЄС також опікується питаннями забезпечення цифрового суверенітету. З цією метою Євросоюз прагне нормативно врегулювати діяльність світових ІТ-корпорацій, оскільки останні 5 років керівні органи Євросоюзу демонтують занепокоєння та активно обговорюють проблему безмежного поширення на ринку європейського континенту американських Інтернет-компаній. Ще у 2018 році Єврокомісія надала поради власникам Інтернет-платформ щодо активізації протидії поширенню незаконного контенту. Заборона поширювалася на: дитячу порнографію, ворожі висловлювання, прояви ксенофобії, пропаганду агресії, інформацію терористичного характеру тощо. За останні 3 роки ЄС вже тричі штрафував "Google" на суму понад 8 млрд. Євро за просування операційної системи "Android" через використання власного пошукового ресурсу, "Apple" підпала під розслідування за нав'язування користувачам iPhone-сервісу "Apple Music", а "Facebook" та "Amazon" були покарані за використання особистих даних користувачів з метою просування власних товарів та послуг. Однак, європейські штрафи та інші санкції фактично не вплинули на американських монополістів.

На початку 2021 року антимонопольні органи ЄС запросили у рекламодавців інформацію про практику "Google" у сфері надання рекламних технологій. На даний час ця транснаціональна компанія стикається з двома розслідуваннями, проведеними ЄС щодо своєї рекламної практики, зосередженими на технологіях і даних. Загальновідомо, що "Google" і "Facebook" разом захоплюють більше половини світового ринку продажів Інтернет-реклами. Обидві компанії в даний час є об'єктом позову США по їх угоді 2018 року, завдяки якій "Facebook" надає клієнтам можливість розмістити рекламу в мережі видавничих партнерів "Google". ЄС також хоче знати, чи отримують рекламодавці знижки при використанні посередників "Google", які дозволяють рекламодавцям або медіа-агентствам купувати рекламу у багатьох джерел.

У грудні 2020 року європейські урядовці обговорили законопроекти ЄС про цифрові послуги та цифрові ринки, які регламентують не лише продаж товарів у мережі Інтернет-онлайн, а й нормативно зачіпають процедури швидкого видалення протиправного контенту – протягом години після отримання такої вимоги. У випадку бездіяльності компанія може отримати колосальний штраф та понести відповідальність. Цими актами передбачається встановлення правил для онлайн-платформ, які зобов'язані розуміти свою роль та значення в європейській онлайн-екосистемі. Законопроектами передбачається штрафувати європейськими регуляторами ІТ-компанії на суму до 10 % глобальної виручки, а у випадку масштабних порушень – примусово її конфіскувати. Зокрема, проект закону про цифрові ринки регулюватиме антимонопольні порушення ІТ-компаній, а інший законопроект присвячений встановленню покарань за публікацію забороненого та деструктивного контенту.

Законопроект про цифрові ринки ЄС запроваджує поняття "страж" (*gatekeeper*) – компанія, статус якої дозволить контролювати платформу, тобто сервіси. Таким чином, передбачається створення природних монополій у сфері цифрової економіки. Типові приклади – магазини додатків "Apple" та "Google". Останнім часом у якості негативних прикладів у документах ЄС фігурували саме "Apple", "Google", "Amazon". Встановлюються вимоги для так званих "стражів": прибуток має складати не менш 6,5 млрд. Євро, а капіталізація – мінімум 65 млрд. Євро. Обов'язки "стража" – забезпечувати усім своїм клієнтам рівні умови роботи, заборона на створення будь-яких преференцій для власних сервісів та використання даних своїх клієнтів. "Стражі" мають узгоджувати з владою навіть дрібні угоди щодо злиття або поглинання, а також у сфері інвестування. Звідси випливає, що запрацюють антимонопольні обмеження. Передбачаються й штрафи щодо ІТ-корпорацій: 6 % від прибутку треба буде заплатити у випадку відмови компанії видаляти контент, який

визнано в ЄС неприпустимим. Акцент зроблено на посиленні податкового законодавства, особливо щодо компаній “Apple”, “Google”, “Facebook”, “Amazon”, які акумулюють великі прибутки, надаючи свої послуги у державах ЄС, хоча сплачують податки за мінімальними ставками, відкриваючи свої штаб-квартири в Ірландії або в Нідерландах. Тому в ЄС для транснаціональних ІТ-компаній обговорюється питання про перехід до сплати ПДВ на територіях надання своїх послуг.

Таким чином, ЄС взяв курс на посилення та зміцнення свого цифрового суверенітету на фоні загострення протистояння між КНР та США. ЄС має намір інвестувати мільярди Євро у власний ІТ-сектор в рамках посилення свого технологічного суверенітету. Тобто європейські лідери планують зменшити залежність від розробок, які надходять з КНР та США, а також значно послабити зарубіжні ІТ-корпорації на власному цифровому ринку. Європейський цифровий суверенітет має бути спрямований на динамічний розвиток власних цифрових навичок, принаймні ключових технологій, не виключаючи присутність інших постачальників. Проте, на переконання провідних експертів, на даний час домінує позиція, згідно з якою ІТ-індустрія є сферою, у якій Європа значно поступається не тільки США, але й Китаю, Японії та навіть Південній Кореї.

За таких умов можна підсумувати, що у ЄС дедалі частіше говорять про цифровий суверенітет, але, швидше, в контексті цифрової безпеки. Загальною потребою для політикума ЄС є необхідність вдосконалити своє законодавство та виробити норми для технологічних компаній і транснаціональних корпорацій, що оперують у діджитал-сфері й активно впливають на повсякденне життя європейських громадян. Таким чином, європейці наголошують на виробленні правил і контролі за доброчесністю з боку засобів масової комунікації як можливих засобів або ж суб’єктів недоброчесних дій стосовно не тільки держави, а й пересічних громадян. На цьому фоні не останнім питанням залишається забезпечення цифрового суверенітету, який включає забезпечення цифрових прав громадян при використанні засобів масової комунікації, зміст якого охоплює не тільки захист персональних даних, а й право розпоряджатися своїми даними.

Ще одним перспективним напрямком захисту цифрового суверенітету вбачається створення вітчизняної операційної системи програмного забезпечення, відмова від використання китайської продукції та відповідних розробок. Так, наприклад, останнім часом відбувалося лобіювання з боку США бойкоту китайській компанії “Huawei” та її продукції, внесення до чорного списку сотні інших китайських технологічних компаній.

Висновки.

В сучасних реаліях контекст пандемії коронавірусу призвів до потреби глобального переосмислення ролі та значення цифрових технологій та практики їх застосування. Довгострокова тенденція загального зростання ринку електронної комерції була підтримана режимом карантину, в умовах масової самоізоляції та чисельного використання соціальних мереж та різноманітних онлайн-платформ. Ще 10 років тому втручання у внутрішні справи держави передбачало агресію та перетинання кордонів. Зараз спричинити шкоду іншій державі реально за допомогою Інтернет-технологій, у зв’язку з чим парламенти держав світу мають забезпечити цифровий суверенітет своїх країн. При цьому з запровадженням цифрових технологій парламенти мають працювати над законами, норми яких спрямовані не тільки на побудову нової економіки, але й врегулювати питання, пов’язані із кібербезпекою та забезпеченням цифрового суверенітету, захисту персональних даних, національного сегменту кіберпростору. Тобто передові держави світу шляхом схвалення відповідного законодавства вживають заходів з метою побудови власної моделі цифрового суверенітету. Підставами для цього

також є тиск на гравців світового ринку з боку зарубіжних ІТ-гігантів, зокрема “Google” та “Facebook”, які отримують колосальні прибутки від своєї діяльності у тій чи іншій державі, хоча не підпадають під національну юрисдикцію та сплачують мінімальні податки.

Набувають неабияких масштабів численні випадки порушення цифрових прав громадян зарубіжними ІТ-компаніями, які демонстративно ігнорують вимоги національного законодавства. Актуальним є збереження цифрового суверенітету, оскільки вже стало практикою соціальних мереж втручатися у справи електронних ЗМІ та блогерів шляхом видалення контенту або блокування цілих каналів. Також збір даних користувачів соціальних мереж має відбуватися тільки за їх згоди, щонайменше користувачі повинні бути поінформовані про те, що дані збираються та акумулюються. Наприклад, мережі “Facebook” та “Twitter” порушують права громадян, оскільки не переносять до національних юрисдикцій держав сервери з даними користувачів. Також “Instagram”, який належить мережі “Facebook”, без пояснень практикує знищення аккаунтів користувачів, порушуючи права на свободу самовираження, на свободу слова, захист персональних даних тощо. У зв’язку із викладеним, обов’язком держави є забезпечення захисту цифрових прав громадян, впровадження заходів з метою входження зарубіжних компаній у правове поле держави та здійснення своєї діяльності виключно у його рамках.

Достатня увага повинна приділятися питанням видалення деструктивного контенту соціальними мережами. На законодавчому рівні доцільно запровадити такі вимоги. Держави мають об’єднатися з метою примусу ІТ-корпорацій встановити прозорі та відкриті правила поведінки соціальних мереж, які у свою чергу, повинні показати свої стандарти модерації, оскільки кожен повинен розуміти – за що його можуть заблокувати, перелік існуючих стоп-слів тощо.

Ефективним механізмом може стати заборона будь-яких угод між державними органами та державних компаній з “Google”, “Facebook” та іншими від розміщення реклами, включаючи закупівлю товарів та послуг. Проте жодне цифрове законодавство не є універсальним засобом від усіх загроз та ризиків, оскільки кордони між реальним та віртуальним життям стерлися, а системна робота над створенням безпечного та відкритого Інтернет-середовища є справою не тільки держави, але й соціальних платформ, які надають відповідні послуги. Сучасне світове законодавство та прискіплива увага до цифрової грамотності населення це переконливо доводять та підтверджують.

Досить перспективним та корисним вбачається турецький досвід, який кардинально змінив ставлення світової спільноти до соціальних мереж, підвищив їхню відповідальність. У світовій практиці достатньо прикладів регулювання Інтернет-сфери, забезпечення цифрового суверенітету, проте для України доцільно враховувати здобутки міжнародного досвіду та нормативно деталізувати власне розуміння цієї проблематики, спрямувати зусилля на розвиток та захист українського сегменту мережі Інтернет. У сучасному глобальному вимірі домінує позиція, що діяльність соціальних мереж становить чималу загрозу національному цифровому суверенітету в будь-якій країні світу. Передумовами для цього стала діяльність транснаціональних гігантів ІТ-індустрії у національних сегментах кіберпростору, яка здійснюється поза межами національної юрисдикції та з порушенням вимог законодавства тієї чи іншої держави. З метою унормування функціонування соціальних мереж, глобальних ІТ-платформ кожна держава розробляє та встановлює законодавчий алгоритм моніторингу та контролю за їх діяльністю, включаючи механізми впливу у вигляді штрафів та санкцій, збільшення податкового навантаження на цих суб’єктів тощо.

Враховуючи викладене, для України є актуальним посилення захисту цифрових прав громадян, одночасно зі створенням передумов для адміністрування податку на додану вартість при оподаткуванні електронних послуг фізичним особам, що постачаються нерезидентами в мережі Інтернет. В Україні результатом тривалих дискусій з приводу запозичення кращих практик європейського та міжнародного досвіду у сфері забезпечення цифрового суверенітету стала підготовка законопроекту "Про внесення змін до Податкового кодексу України щодо оподаткування податком на додану вартість електронних послуг, що постачаються нерезидентами фізичним особам, місце постачання яких розташовано на митній території України" від 19.12.19 р. № 2634 (так званий "податок на "Google") [8]. Ще наприкінці 2020 року депутати обговорювали можливість оподаткування доходів "Google", "Netflix", та "Amazon", а також компаній, що продають відео, музику, рекламу, ігри та доступ до Хмарних сервісів.

17 лютого 2021 року Верховна Рада України прийняла за основу відповідний законопроект, а 8 квітня 2021 року він був схвалений. Положеннями законопроекта передбачено: механізм оподаткування податку на додану вартість нерезидентами; можливість сплачувати податок у валюті, фактично не перебуваючи на території України. Завдяки цьому закону буде запроваджений дієвий механізм, який зобов'яже світових гігантів ("Google", "Facebook" тощо), які працюють в Україні, сплачувати податки до бюджету, що дозволить урівняти в правах український бізнес і бізнес транснаціональний, який чомусь сьогодні є пільговим. Також доцільно у вітчизняному законодавстві визначити поняття "іноземна соціальна мережа", її правове становище, податковий режим тощо.

Використана література

1. Декларація про Державний суверенітет України від 16 липня 1990 року. URL: https://zakon.rada.gov.ua/laws/show/55-12#Text (дата звернення: 02.04.2021).

2. Дмитренко М. Проблемні питання інформаційної безпеки України 2018. URL: https://journals.iir.kiev.ua/index.php/pol_n/article/download/3318/2997 (дата звернення: 02.04.2021).

3. Довгань О.Д. Національний інформаційний суверенітет – об'єкт інформаційної безпеки. *Інформація і право*. № 3(12)/2014. С. 102-112.

4. Доронін І.М. Правові проблеми суверенізації Інтернету. *Інформація і право.* № 2(29)/2019. С. 74-81.

5. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право.* 2016. № 1. С. 17-23.

6. Солодка О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс. *Інформація і право.* № 1(32)/2020. С. 80-87.

7. Internet ortaminda yapilan yayinlarin düzenlenmesi ve bu yayinlar yoluyla işlenen suçlarla mücadele edilmeSİ Kabul Tarihi: 29.07.2020. URL: http://www.lebibyalkin.com.tr/mevzuat/mevzuattaki-son-degisiklikler/2020-mevzuattaki-son-degisiklikler_temp_temp-000_/2020-temmuz_temp_temp-000_2020_07 (дата звернення: 02.04.2021).

8. Щодо оподаткування податком на додану вартість електронних послуг, що постачаються нерезидентами фізичним особам, місце постачання яких розташовано на митній території України: проект закону про внесення змін до Податкового кодексу України від 19.12.19 р. № 2634. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67703 (дата звернення: 02.04.2021).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~