УДК 35.746.1
DOI https://doi.org/10.32782/2524-0374/2023-9/67

ДОСВІД ЄС ТА НАТО У ПИТАННЯХ ВДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОГО ЗАКОНОДАВСТВА

EXPERIENCE OF THE EU AND NATO IN IMPROVING INFORMATION LEGISLATION

Солодка О.М., к.ю.н., с.н.с.

У статті досліджуються особливості взаємодії держав у глобальному інформаційному в межах ЄС та НАТО просторі та правова основа цієї взаємодії з огляду на присутність інформації у всіх сферах державного та міждержавного рівня, що вимагає вжиття необхідних заходів та розроблення правових основ.

Проведене дослідження засвідчує те, що питання правового унормування інформаційних відносин набувають особливого значення в рамках ЄС, існують тісні зв'язки інформаційної безпеки із загальною політикою безпеки ЄС, а ключовими питаннями ЄС у контексті забезпечення інформаційної взаємодії держав є правове регулювання захисту персональних даних, побудова цифрового суверенітету ЄС, протидія дезінформації та меседжам ненависті в Інтернеті, технологічний розвиток (штучний інтелект).

Положення стандартів НАТО направлені, в першу чергу, на об'єднання великої кількості правових норм країн – членів Альянсу, деякі принципи можливо застосувати для об'єднання (налагодження обміну інформацією) між інформаційними системами різних структур. Важливим також є кіберпростір в тому сенсі, що – це набагато більше, ніж просто Інтернет, адже усі пристрої доступні через кіберпростір можуть бути потенційними цілями та потенційними загрозами. До цього постійно зростаючого переліку додається використання Інтернету речей.

Проте вищеозначені положення стосуються більшою мірою членів зазначених організацій. Відтак, у перспективі доцільним видається добровільне вироблення норм безпечного співіснування держав в інформаційному просторі в багатосторонньому або двосторонніх форматах. Також мова може йти про підписання рамкових міжнародних угод щодо встановлення загальних принципів забезпечення міжнародної безпеки в інформаційній сфері. У довгостроковій перспективі доцільно виробити комплекс зобов'язань щодо відповідальної поведінки держав та інших суб'єктів в інформаційному просторі.

Ключові слова: глобальний інформаційний простір, інформаційний простір, інформація, інформаційне суспільство.

The article deals with the peculiarities of the interaction of states in the global information space within EU and NATO and the legal basis of this interaction are investigated, given the presence of information in all spheres of the state and interstate level, which requires taking the necessary measures and development of legal frameworks.

The conducted research proves that the issue of legal regulation of information relations acquires special importance within the framework of the EU, there are close ties between information security and the general security policy of the EU, and the key issues of the EU in the context of ensuring the information interaction of states are the legal regulation of the protection of personal data, the construction of the digital sovereignty of the EU, countering misinformation and hate messages on the Internet, technological development (artificial intelligence).

The provisions of NATO standards are aimed, first of all, at the unification of a large number of legal norms of the member countries of the Alliance, some principles can be applied to unification (establishment of information exchange) between information systems of different structures. Cyberspace is also important in the sense that it is much more than just the Internet, as all devices accessible through cyberspace can be potential targets and potential threats. Adding to this ever-growing list is the use of the Internet of Things.

However, the above-mentioned provisions apply to a greater extent to the members of the mentioned organizations. Therefore, in the future, it seems expedient to voluntarily develop norms for the safe coexistence of states in the information space in multilateral or bilateral formats. It can also be about signing framework international agreements on establishing general principles for ensuring international security in the information sphere. In the long term, it is advisable to develop a set of obligations regarding the responsible behavior of states and other subjects in the information space.

Key words: global information space, information space, information, information society.

Постановка проблеми. Окінавська хартія інформаційного суспільства стала документом, у якому світова спільнота визнала міжнародну інформаційну безпеку необхідною умовою існування людства, закликаючи до розробки спільної стратегії побудови інформаційного суспільства, і цей факт на сьогодні не викликає сумнівів, адже безпрецедентний розвиток науково-технічного прогресу в галузі телекомунікаційних технологій призвів до виникнення практично необмежених можливостей протиправного використання інформаційного простору з метою отримання переваг у конкурентній боротьбі всіх рівнів, зокрема шляхом маніпулювання свідомістю індивідів за допомогою поширення дезінформації, протиправного заволодіння інформацією з обмеженим доступом, посягання на державні інформаційні ресурси тощо.

Транскордонний характер інформаційних технологій, їх доступність, анонімність користувачів ускладнюють вирішення проблеми. Крім того, у багатьох країнах велика частина критично важливих інформаційних ресурсів, мереж і систем знаходиться в приватній власності, а в умовах постійного динамічного розвитку інформаційних технологій постійно з'являються нові види інформаційної зброї, шкідливого програмного забезпечення, вірусних атак тощо.

Характеризуючи поняття «інформаційне суспільство», на нашу думку, слід брати до уваги два взаємопов'язані компоненти надзвичайну значущість інформації для суспільства та індивідів, яка завжди відігравала ключову роль у забезпеченні їх стабільного функціонування та розвитку, та невіддільність інформаційних технологій, що породжує нові завдання, зважаючи на транскордонність інформаційного простору – на наднаціональному рівні.

Аналіз останніх досліджень і публікацій. У сучасній науковій літературі питання правового унормування інформаційних правовідносин на міжнародному рівні відображено у наукових працях І. Арістової, О. Баранова, О. Довганя, Б. Кормича, Є. Макаренко, В. Пилипчука, О. Олійника, О. Тихомирова, В. Цимбалюка, М. Швеця та багатьох інших, проте розвиток інформаційної сфери вимагає перманентного дослідження означених питань з метою вироблення адекватних сучасності правових заходів безпеки.

Метою статті є виокремлення напрямів діяльності ЄС та НАТО в питаннях правового врегулювання інформаційних правовідносин.

Виклад основного матеріалу. Сьогодні більшість дослідників ролі інформаційно-комунікаційних технологій в житті світової спільноти розглядають глобальний інформаційний простір як сукупність інформаційних ресурсів і інфраструктур, які складають державні і міждержавні комп'ютерні мережі, телекомунікаційні системи та мережі загального користування, інші транскордонні канали передачі інформації.

Міжнародна інформаційна безпека визначається як взаємодія акторів міжнародних відносин з операцій підтримання сталого миру на основі захисту міжнародної інфосфери, глобальної інфраструктури та суспільної свідомості світової спільноти від реальних і потенційних інформаційних загроз [1].

У глобальному вимірі правова основа функціонування інформаційного суспільства повинна гарантувати стабільність його стабільнсть, однак бути достатньо гнучкою, відображати зміни, викликані технічним прогресом. Крім того, нормативно-правове забезпечення суспільних відносин у глобальному інформаційному суспільстві має бути стандартизованим, впроваджуючи глобальний регуляторний механізм, оскільки фрагментація нормативно-правового регулювання інформаційного суспільства на рівні національних правових систем може сприяти утворенню декількох центрів впливу та дискримінаційному становищу менш впливових політичних акторів.

Відповідні паралелі можливо провести, досліджуючи діяльність Європейського союзу (ЄС) в інформаційній сфері. Так, формування єдиного цифрового простору рамках ЄС почалося з прийняттям Єврокомісією у 2015 році Стратегії Єдиного цифрового ринку ЄС [2], в рамках якої цифрова інтеграція ЄС передбачає три «стовпи» (напрямки) політики і, відповідно, правового регулювання: забезпечення якісного онлайн-доступу до цифрових послуг і товарів; формування цифрового середовища для розвитку цифрових послуг і цифрових мереж; розвиток цифровізації як драйвера зростання єдиної європейської економіки.

Глобалізація породжує нових суб'єктів правовідносин, які є більш потужними, ніж окрема держава – транснаціональні корпорації мають можливість суттєво впливати на всі сфери суспільного життя, не виключенням є інформаційна. Окрім цього, сьогодні інформаційно-комп'ютерні технології являють собою багаторівневу мережу, глобальна технологічна інфраструктура якої забезпечує їх транскордонне функціонування і використання, що підлягає врахуванню при правовому регулюванні інформаційних правовідносин.

В Європейському Союзі актуальним є питання захисту персональних даних: аналітики звертають увагу, що транснаціональні компанії (Google, Apple, Facebook, Amazon, Microsoft) збирають величезні обсяги персональних даних для просування реклами, які до того ж можна використати з метою формування політичних уподобань, просування потрібних ідей. У 2016 році ЄС був введений в дію Загальний регламент захисту персональних даних (General Data Protection Regulation – GDPR) [3], на підставі якого зокрема, користувачі Інтернету мають право знати, які дані збираються під час відвідування певного веб-сайту. Регламент також вимагає, щоб дані цих користувачів не виходили за межі ЄС у будь-якому вигляді.

Наразі у держав-членів ЄС відсутнє «колективне» усвідомлення кіберзагроз, що пов'язано з тим, що національні органи влади систематично не обмінюються інформацією (на відміну від приватного сектора), яка може допомогти оцінити стан кібербезпеки в ЄС. Держави-члени повідомляють лише про частину інцидентів, а обмін інформацією не є систематичним чи всебічним; кібератаки можуть бути лише одним із аспектів узгоджених зловмисних атак, направлених проти європейських держав-членів. Наразі взаємодопомога між державами-членами обмежена, а для держав-членів та установ і органів ЄС не існує жодного оперативного механізму на випадок виникнення масштабних, транскордонних кіберінцидентів або кризи.

Щоб гарантувати, що всі країни зможуть скористатися соціальними, економічними та політичними вигодами від Інтернету та використання технологій, ЄС продовжує підтримувати своїх партнерів для підвищення їхньої стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози.

В світлі цього ухвалено Стратегію кібербезпеки ЄС на цифрове десятиліття [4], яка є ключовим компонентом формування цифрового майбутнього Європи, Плану Єврокомісії щодо відновлення Європи, Стратегії Союзу безпеки на 2020–2025 роки, Глобальної стратегії зовнішньої політики та політики безпеки ЄС та Стратегічного порядку денного Європейської Ради на 2019–2024 роки та визначає яким чином ЄС захищатиме своїх громадян, підприємства та установи від кіберзагроз, і як сприятиме міжнародній співпраці та стане лідером у забезпеченні глобальної та відкритої мережі Інтернет. Стратегія спрямована на забезпечення глобальної та відкритої мережі Інтернет із потужним захистом для запобігання виникнення ризиків для безпеки та основних прав і свобод людей у Європі. Враховуючи прогрес, досягнутий під час виконання попередніх стратегій, вона містить конкретні пропозиції щодо розгортання трьох основних інструментів – регуляторного, інвестиційного та політичного – для застосування у трьох сферах діяльності: ЄС:

1) стійкість, технологічний суверенітет та лідерство,

2) нарощування оперативного потенціалу для запобігання, стримування та реагування,

3) забезпечення глобального та відкритого кіберпростору.

Стратегія також має на меті встановити пріоритети в галузі розвитку штучного інтелекту, оскільки дана сфера в даний час розвивається найбільш стрімко і являє собою непередбачену і потенційно небезпечну технологію, пропонуючи певний баланс між державними гарантіями збереження персональних даних з одного боку та розвитком систем штучного інтелекту – з іншого.

Отже, в цілому цифрова політика ЄС спрямована на консолідацію інформаційних ресурсів країн-членів. Це відповідає світовому тренду на фрагментацію і суверенізацію кіберпростору, однак саме у випадку з ЄС має унікальну специфіку, адже в ЄС, крім національного рівня, суверенізація має ще один вимір – регіональний.

Важливим також є прийняття Закону ЄС про цифрові послуги (Digital Services Act), основними завданнями якого є: удосконалити механізм захисту прав користувачів в Інтернеті; захистити від небажаної реклами; скоротити кількість нелегального контенту в Інтернеті, покращити умови для запуску та розширення цифрових послуг для учасників онлайн-ринку в ЄС; збільшити прозорість онлайн-платформ, зокрема, щодо алгоритмів, які використовуються для реклами; запобігти зловживанням «інтернет-владою» з боку надвеликих платформ, які охоплюють аудиторію в понад 10% населення ЄС; сприяти зростанню і розширенню невеликого бізнесу та залученню нових учасників онлайн-ринку; впровадити систему зобов'язань та відповідальності, а також звільнення від відповідальності для забезпечення прав споживачів цифрових послуг. Закон має за мету забезпечити захист основних прав користувачів Інтернету, впроваджує безпрецедентний стандарт відповідальності онлайн-платформ щодо незаконного та шкідливого вмісту, а також визначає єдиний набір правил на внутрішньому ринку, сприяючи конкуренції.

ЄС активно протидіє дезінформації: у 2016 р. було прийнято документ «Спільні рамки протидії гібридним загрозам – відповідь Європейського Союзу» («Joint Framework on countering hybrid threats – a European Union response») [5], в якому зазначалося, що «масові дезінформаційні кампанії, використання соціальних медіа для контролю політичного наративу, радикалізації, вербування осіб, можуть бути засобами поширення гібридних загроз» та мало на меті сприяти цілісному підходу, який дозволить ЄС у координації з державами-членами конкретно протидіяти загрозам гібридного характеру. В контексті цього у 2018 році було опубліковано саморегулюючий «Кодекс поведінки з протидії дезінформації» (Code of Practice on Disinformation) [6], в якому визначено питання, пов'язані

з формуванням основи для структурованого діалогу та протидії дезінформації в Інтернеті, який підписали представники найбільших інтернет-платформ та соціальних медіа (Google, Facebook, Twitter та Mozilla).

Ще одним важливим кроком щодо протидії дезінформації в європейському інформаційному просторі стало прийняття у 2018 р. «Плану дій щодо протидії дезінформації» (Action Plan against Disinformation) [7] в Європі та поза його межами з акцентуванням на чотирьох ключових сферах: вдосконалення можливостей установ ЄС виявляти, аналізувати та викривати дезінформацію; посилення скоординованих та спільних реакцій на дезінформацію; мобілізації приватного сектору у боротьбі з дезінформацією; підвищення обізнаності та підвищення стійкості суспільства.

Отже, вище викладене засвідчує те, що питання правового унормування інформаційних відносин набувають особливого значення в рамках ЄС, існують тісні зв'язки інформаційної безпеки із загальною політикою безпеки ЄС, що відображено в кібереелементах Стратегії безпеки ЄС на 2020 рік та у Програмі боротьби з тероризмом ЄС [8], а ключовими питаннями ЄС у контексті забезпечення інформаційної взаємодії держав є правове регулювання захисту персональних даних, побудова цифрового суверенітету ЄС, протидія дезінформації та меседжам ненависті в Інтернеті, технологічний розвиток (штучний інтелект).

Це відображає загальну тенденцію стурбованості Євросоюзу не стільки з приводу «м'якої сили» та ідеологічної боротьби з боку інших країн, скільки з приводу необхідності вдосконалити своє законодавство та виробити норми для технологічних компаній і транснаціональних корпорацій, що оперують у цифровій сфері, а відтак – справляють значний вплив повсякденне життя громадян країн Євросоюзу. То ж головним акцентом у європейській інформаційній політиці є вироблення правил і контроль за доброчесністю з боку засобів масової комунікації як можливих засобів або ж суб'єктів недоброчесних дій стосовно не тільки держави, а й пересічних громадян). При забезпеченні цифрового суверенітету також важливим є забезпечення прав громадян при використанні засобів масової комунікації, включно не тільки із захистом персональних даних, а й правом розпоряджатися своїми даними і обмежувати їх поширення без згоди автора [9].

Нормативно-правові акти, прийняті на рівні НАТО у сфері забезпечення інформаційної безпеки, можна умовно розподілити на дві групи:

– міжнародні стандарти, які на державному рівні визнаються усіма країнами-членами НАТО, і використання яких спрямоване на забезпечення інтероперабельності;

– власне документація НАТО – стандарти, положення та правила, які встановлюють мінімальні вимоги щодо забезпечення захисту інформації на встановленому рівні.

Положення стандартів НАТО направлені, в першу чергу, на об'єднання великої кількості правових норм країн-членів Альянсу, деякі принципи можливо застосувати для об'єднання (налагодження обміну інформацією) між інформаційними системами різних структур, зокрема, об'єднавши розвідувальну, тактичну, стратегічну інформацію, оперативну інформацію військових підрозділів різних родів військ та правоохоронних органів, МНС, метеорологічних служб тощо за допомогою механізму захищеного зв'язку.

Одним з найновіших чинних стандартів НАТО у сфері забезпечення інформаційної безпеки є AJP-3.20 «Спільна доктрина щодо операцій у кіберпросторі» – Allied Joint Doctrine for Cyberspace Operations, опублікована у 2020 році [10]. У Доктрині, зокрема, зазначається, що вільний потік даних і безперебійне функціонування мереж стало критичним для функцій та послуг громадянського суспільства та військових сил, а державні та недержавні суб'єкти прагнуть використати вразливі місця військових та невійськових інформаційних систем для проникнення, пошкодження чи знищення даних або для отримання престижу, політичних чи військових переваг або прибутку. Тож цифрові мережі та системи потрібно захистити від пошкодження інформації. У взаємопов'язаному світі, де військовий успіх може залежати не стільки від створення фізичних наслідків, скільки від контролю наративів, свобода дій у віртуальному просторі може бути такою ж важливою, як контроль над землею, повітрям, космосом або морем.

Також наголошується на тому, що кіберпростір – це набагато більше, ніж просто Інтернет, адже усі пристрої доступні через кіберпростір, тож можуть бути потенційними цілями та потенційними загрозами. До цього постійно зростаючого переліку додається використання Інтернету речей. Інформаційний простір включає власне інформацію, осіб, організації та системи, які отримують, обробляють та передають інформацію, а також когнітивний, віртуальний та фізичний простір, в якому це відбувається. За останні роки в цьому середовищі відбулися значні зміни, тож важливість поширення в усьому світі інформації, швидкість, з якою інформація розповсюджується, роль соціальних медіа та надійність інформаційних систем створили ситуацію, коли жодне рішення або дії Альянсу не можуть бути вжиті, не враховуючи їх потенційний вплив на інформаційне середовище або ж вплив інформаційного середовища на ці рішення. Зазначається, що вразливість у кіберпросторі пов'язана з її залежністю від кіберпростору. Відтак, Альянс повинен мати можливість протистояти супротивникам та підтримувати власні операції, оскільки можливості продовжують розвиватися та вдосконалюватися.

Висновки. Сьогодні як ніколи держави мають гостру потребу у виробленні ефективної політики забезпечення безпеки своїх національних інтересів в інформаційній сфері, яка повинна враховувати об'єктивні реалії сучасного інформаційного середовища. У результаті глобальної інформатизації формується нове середовище безпеки і нові виклики, на які держави змушені реагувати. Багато з них мають внутрішній характер, хоча і є наслідком кіберпростору, який за своєю природою є транснаціональним. Зростає список загальних, що стоять перед усіма державами, викликів та загроз інформаційному простору, який стає основою для спільної протидії, що підтверджено дослідженням досвіду ЄС та НАТО у цій сфері.

При розробленні концепцій переходу до інформаційного суспільства використовується комплексний підхід, заснований на підтримці балансу інтересів людини і держави, а формування глобального інформаційного суспільства відбувається під впливом прогресу нових інформаційних і телекомунікаційних технологій у поєднанні з глобалізацією ринків, тому для гармонійного входження в інформаційне суспільство та дотримання необхідного балансу необхідні координуючі зусилля на міжнародному рівні, відповідно міжнародні правові ініціативи, оскільки врегулювання інформаційних правовідносин виключно на національному рівні не є адекватним загрозам, що створює розвиток сучасного інформаційного суспільства. Зазначене підтверджено активізацією питань удосконалення інформаційного законодавства в рамках ЄС та НАТО та є визначним для врахування в законодавстві країн, які не є членами цих міжнародних організацій.

ЛІТЕРАТУРА

1. Макаренко Є.А. Міжнародна інформаційна політика: структура, тенденції, перспективи: дис... д-ра. політич. Наук : 23.00.04 / Націон. ун-т ім. Т.Шевченка. К., 2003. 475 с.

2. Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=celex%3A52015DC0192 (дата звернення 18.09.23)

3. General Data Protection Regulation – GDPR. URL: https://gdpr-info.eu/(дата звернення 14.09.23)
4. The EU's Cybersecurity Strategy for the Digital Decade. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Brussels, 16.12.2020 JOIN (2020) 18 final. URL: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 (дата звернення 22.08.23)
5. Joint communication to the European parliament and the council: Joint Framework on countering hybrid threats a European Union response. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX% 3A52016J C0018 (дата звернення 12.09.23)
6. The 2022 Code of Practice on Disinformation. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. (дата звернення 24.08.23)
7. Action Plan against Disinformation URL: https://www.eeas.europa.eu/node/54866_en. (дата звернення 17.09.23)
8. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond, 09.12.2020 p., COM (2020) 795. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0795 &qid= 1631885972581(дата звернення 15.09.23)
9. О. Шульга. Цифровий суверенітет і українське суспільство Час для дискусії настав. URL: https://dt.ua/gazeta/issue/1232(дата звернення: 11.01.2023).
10. Allied Joint Doctrine for Cyberspace Operations. Jan.2020. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf. (дата звернення 14.08.23)