DOI https://doi.org/10.30525/978-9934-26-277-7-261

INTERNATIONAL LEGAL PRINCIPLES OF ENSURING CYBER SECURITY OF THE USE OF INFORMATION TECHNOLOGIES

МІЖНАРОДНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Tchitchagua S.
Academy of Labour, Social Relations and Tourism
Kyiv, Ukraine

Чічагуа С.
Академія праці, соціальних відносин і туризму
Київ, Україна

Одним із головних цивілізаційних трендів розвитку суспільства у XXI столітті стала технологічна інформаційно-комунікаційна модернізація усіх сфер суспільного життя, що значно відобразилось на організації функціонування вищої освіти та науки. За останні кілька років цифровізація стрімко увійшла у повсякдення та фактично визначила сенс новітньої епохи нашого буття. Цифрові технології вже є складовою приватного життя практично кожної людини, забезпечують інноваційну систему публічного управління, інформаційно-комунікаційні зв'язки демократично організованого суспільства, виступають детермінантою інфраструктурного переоснащення, підвищення конкурентоспроможності національної економіки, поглиблення світових глобалізаційних процесів.

Тож, сучасні інформаційні технології докорінно змінюють життя кожного, а відповідно – систему суспільних відносин, що вимагає належного законодавчого реагування – перетворення цифрової реальності у правову – з метою забезпечення реалізації прав і законних інтересів людини. Безумовно, на сьогодні перспективним убачається формування правової політики, спрямованої на процеси цифровізації життя людини. За таких умов постають закономірні та логічні питання щодо забезпечення кібербезпеки в цифровому світі та її нормативно-правове забезпечення.

Сучасна система принципів у сфері кібербезпеки є спільним надбанням людської цивілізації та становить тривалий процес, пов'язаний із виникненням, формуванням та сучасним розумінням системи керівних ідей застосування міжнародно-правових актів та

національного законодавства у сфері кібербезпеки. Спочатку вони зароджувалися як певні фундаментальні начала, уявлення, що зображають демократичні цінності у сфері реалізації права на кібербезпеку, що має на меті мету уникнення порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів, забезпечення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем тощо.

З огляду на нетривалу історію правового регулювання кібербезпеки у міжнародному праві, система відповідних принципів ще не є усталеною та перебуває на етапі формування і у 1999 року вперше вносилося до глобального порядку денного у Резолюції ООН 53/70 «Розвиток у галузі інформації та телекомунікацій у контексті міжнародної безпеки». Так, з огляду на потребу запобігання зловживанню та протизаконній експлуатації інформаційних ресурсів або технологій ООН закликала держави-члени висловити власну позицію, зокрема, щодо доцільності розробки міжнародних принципів, які б підвищили глобальну безпеку інформаційних та телекомунікаційних систем та допомогли б боротися з інформаційним тероризмом й злочинністю [1].

Серед міжнародно-правових принципів забезпечення кібербезпеки науковці [2] виокремлюють ті, що безпосередньо чи опосередковано визначено у актах міжнародного права, а також ті, що формулюються фахівцями-правниками, юристами-міжнародниками в означеній сфері, здебільшого мають доктринальний характер. Стратегія кібербезпеки ЄС закріплює п’ять відповідних принципів:

– основні цінності ЄС використовуються як у цифровому/ віртуальному, так й матеріальному/реальному світі (*in the digital as in the physical world*);

– захист основних прав, свободи висловлення поглядів, персональних даних та конфіденційності відображає взаємозалежність між безпечним Інтернет-простором та правами людини. Так, кібербезпека може бути надійною та ефективною, якщо вона ґрунтується на основних правах та свободах, які закріплено Хартією основних прав ЄС, та цінностях ЄС [3]. Водночас права людини не можуть бути забезпечені без безпечних інформаційних мереж та систем. Процедури міждержавного обміну задля забезпечення кібербезпеки тією інформацією, що містить персональні дані, мають

відповідати законодавству ЄС про захист даних та враховувати права фізичних осіб у цій сфері;

– доступ для всіх передбачає, з огляду на масштаб цифровізації суспільних відносин, можливість кожного мати доступ до Інтернету та до безперешкодного потоку інформації / unhindered flow of information [4]. Гарантії цілісності Інтернету/ the Internet's integrity – незмінності збережених даних в інформаційній системі і під час їхньої передачі – та безпеки є умовами забезпечення безпечного доступу для всіх;

– демократичне та ефективне управління за участі багатьох суб'єктів / multi-stakeholder governance [5] є актуальною потребою, бо в сучасному світі повсякденною діяльністю з управління Інтернет-ресурсами займається декілька заінтересованих сторін, серед яких багато комерційних компаній та неурядових організацій. З урахуванням відповідних реалій ЄС визнає значущість усіх зацікавлених сторін у сучасній моделі управління Інтернетом та підтримує такий підхід [6];

– спільна відповідальність щодо забезпечення кібербезпеки генерується постійним зростанням залежності людини від ІКТ у всіх сферах, що зумовлює наявність певних вразливостей, які слід правильно визначити, ретельно проаналізувати, ліквідувати або зменшити. Усі суб'єкти цифрових відносин – органи державної влади та місцевого самоврядування, приватний сектор чи окремі громадяни – мають визнати спільну відповідальність та здійснювати власні заходи щодо кібербезпеки, а також за потреби забезпечити скоординовану реакцію для посилення захисту у цій сфері [7].

Серед основних міжнародно-правових принципів, що закріплені у низці актів: Статут ООН [8], Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту ООН, яку ухвалено Генеральною Асамблеєю ООН 1970 року [9], а також Заключний акт Наради з безпеки і співробітництва в Європі 1975 року, а саме Декларація принципів, якими держави-учасники керуватимуться у взаємних відносинах – становлять підґрунтя галузевих та міжгалузевих міжнародно-правових принципів, зокрема у сфері кібербезпеки.

Так, до основних принципів міжнародного права, як відомо, належать – незастосування сили чи погрози силою; територіальної цілісності держав; непорушності державних кордонів; рівноправності й самовизначення народів; мирного розв'язання міжнародних спорів; поваги і захисту прав та основних свобод людини; добросовісного виконання міжнародних зобов'язань; суверенної рівності держав;

невтручання у внутрішні справи держав; міжнародного співробітництва [10].

До другої групи міжнародно-правових принципів щодо кібербезпеки можна зарахувати, зокрема і ті, що виокремлено Гарольдом Хонджу Кохом (Harold Hongju Koh), у доповіді «Міжнародне право у кіберпросторі», проголошеній 18 вересня 2012 року під час юридичної конференції та опублікованій у журналі «Harvard International Law Journal Online» [11]. З урахуванням засад міжнародного гуманітарного права автор пропонує такі принципи реагування держави на мережеві атаки: розрізнення/розмежування та пропорційність. У доповіді розглядається регулювання застосування кіберінструментів у контексті збройного конфлікту та зауважується на важливості розрізнення військових та невійськових цілей, а також заборони мережевих атак, які можуть спричинити випадкову загибель або поранення цивільних осіб, руйнування цивільних об'єктів, що було б надмірним стосовно конкретних та прямих переваг, які очікуються [11]. Крім цього, Гарольдом Хонджу Кохом наголошується на юридичній відповідальності держав за діяльність/дії передбачуваних приватних суб'єктів, що діють за вказівкою держави або під її керівництвом чи контролем [11].

Варто наголосити,що принципи, закріплені Стратегією кібербезпеки ЄС, у тій чи іншій формі містяться у інших міжнародних актах, ухвалених після 2013 року: Висновках Ради ЄС «Стійкість, стримування та оборона: розбудова міцної кібербезпеки для ЄС» від 20 листопада 2017 року підтверджується позиція європейської спільноти щодо відстоювання прав людини, а також акцентується на важливості залучення всіх зацікавлених сторін до керування Інтернетом, зокрема, науковців, громадянського суспільства, приватних підприємців [12]; про потребу ширшої участі неурядових організацій країн-учасниць в якості лідерів та консультантів профільних органів ЄС, що опікуються питаннями протидії дезінформації, зауважується у Резолюції ПАРЄ 2326 (2020) від 31 січня 2020 року «Демократія зламана? Як реагувати?» [13]. Європейській комісії та Цільовим групам зі стратегічних комунікацій Європейської служби зовнішніх зв'язків пропонується спільно, прозоріше та регулярніше обмінюватися інформацією з неурядовими організаціями, що сприятиме підвищенню якості виявлення та аналізу дезінформації задля загального блага

Глобалізаційні процеси, невпинна діджиталізація сприяють множенню викликів для кібербезпеки, що актуалізує розроблення та

ухвалення концептуальних документів для її забезпечення, які з одного боку, ґрунтуватимуться на означених вище міжнародно-правових принципах, а з іншого продукуватимуть нові засади у відповідній сфері.

Література:

1. Resolution Adopted by the General Assembly 53/70. (1999). Developments in the field of information and telecommunications in the context of international security. URL: https://undocs.org/pdf?symbol=en/a/res/53/70

2. «Цифрова Україна»: конституційно-правова модель : колективна монографія / за заг. ред. Р. О. Стефанчука, О. Л. Копиленка, Є. Р. Бершеди, О. М. Клименко. К. : Інститут законодавства Верховної Ради України, 2021. 688 с.

3. Charter of fundamental rights of the European Union (2000/C 364/01). URL: https://www.europarl.europa.eu/charter/pdf/text_en.pdf

4 Про безперешкодний потік інформації йдеться, наприклад, у Маніфесті ІФЛА про Інтернет (прийнятий Сесією Ради ІФЛА 23 серпня 2002 р.). URL: http://ube.nlu.org.ua

5. Malcolm J. Multi-stakeholder Governance and the Internet Governance Forum.Terminus Press, 2008. 611 p.

6. COM(2009) 277, Communication from the Commission to the European Parliament and the Council on «Internet Governance: the next steps». URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0277:FIN:EN:PDF

7. (Joint Communication to European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cyber security Strategy of the European Union: An Open, Safe and Secure Cyberspace (COM JOIN (2013) 1 final). URL: http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

8. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text

9. Декларація про принципи міжнародного права, що стосуються дружніх відносин та співробітництва між державами відповідно до Статуту Організації Об'єднаних Націй : Резолюція 2625 (XXV) Генеральної Асамблеї ООН від 24 жовтня 1970 р. URL: https://zakon.rada.gov.ua/laws/show/995_569#Text

10. Viñuales Jorge E. «Introduction: The Fundamental Principles of International Law – An Enduring Ideal?». In: The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law / edited by Jorge E. Viñuales, 1–11. Cambridge: Cambridge University Press, 2020. URL: https://doi.org/10.1017/9781108652889.001.

11. Koh H.H. International Law in Cyberspace. Remarks as Prepared for Delivery by Harold Hongju Koh to the USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, Sept. 18, 2012. Harvard International Law Journal Online. Vol. 54. URL: https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speechto-Publish1.pdf

12. Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU – Council conclusions (20 November 2017). URL: https://www.consilium.europa.eu/media/31666/st14435en17.pdf

13. Resolution 2326 (2020) Democracy hacked? How to respond? URL: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28598&lang=en16